

情報処理

2021
4

Vol.62 No.4
通巻 673 号

特集 **オンライン** 面白いぞ量子技術

解説 **オンライン** 「情報教育課程の設計指針」解説



巻頭コラム

誰一人取り残さないために情報技術が果たす役割
浅川智恵子

教育コーナー：べた語義

連載：5分で分かる!!有名論文ナメ読み/情報の授業をしよう!/先生、質問です!/ビブリオ・トーク
会議レポート

電子版もご覧ください



電子版を読む (会員無料)
情報学広場



iPhoneなどで読む (有料)
Kindle



電子版を購入 (有料)
Fujisan



Web公開 (無料/有料)
note

IT研究者のひらめき本棚

ビブリオ・トーク：私のオススメ

2017年9月発売 定価 1,980円(本体1,800円+税)

編：情報処理学会 会誌編集委員会

判型 A5変 152頁 ISBN 978-4-7649-0548-1 C3004

月刊『情報処理』の人気連載をまとめた本がついに登場！



情報処理学会誌『情報処理』で好評連載中の「ビブリオ・トーク -私のオススメ-」がついに一冊の書籍に！

この連載でIT研究者の方々が紹介した、デマルコやカーニハン、ヘネシー&パターンソン、更にはアシモフやホーガン、伊藤和典、というバラエティに富んだラインナップを40本収録。

序文は、第一回担当である人工知能研究者・中島秀之。

さらに帯に、メディアアーティスト・落合陽一の推薦文をいただき、IT研究者を目指す学生にもオススメの一冊！

■紹介書籍(一部)

- ◇ ハッカーと画家
- ◇ プログラム書法(第2版)
- ◇ Computer Networks 5th Edition
- ◇ デジタル作法
- ◇ 珠玉のプログラミング
- ◇ Computer Architecture, 5th Edition A Quantitative Approach
- ◇ Operating Systems Design and Implementation (3rd Edition)

- ◇ 機動警察パトレイバー風速40メートル
- ◇ ピープルウェア 第3版
- ◇ Computer Lib / Dream Machines
- ◇ 未来の二つの顔
- ◇ 生体用センサと計測装置(ME教科書シリーズ)
- ◇ Cooking for Geeks—料理の科学と実践レシピ
- ◇ ハッカーのたのしみ

- ◇ ぼくの命は言葉とともにある(9歳で失明18歳で聴力も失ったぼくが東大教授となり、考えてきたこと)
- ◇ 部分と全体 私の生涯の偉大な出会いと対話
- ◇ 夜明けのロボット(上)(下)
- ◇ ポスト・ヒューマン誕生
- ◇ 理科系の作文技術
- ◇ 現代倫理学入門
- ◇ を含む40銘柄を紹介。

※ご注文は、お近くの書店様へ

□ お問合せ先

〒162-0843 東京都新宿区市谷田町2-7-15

株式会社近代科学社 営業部 TEL 03-3260-6161 / FAX 03-3260-6059

sales-corporate@kindaikagaku.co.jp

http://www.kindaikagaku.co.jp

とめ 株式会社とめ研究所

～知能情報処理技術をコアコンピタンスとした
ソフトウェア研究開発受託会社～

- ◆情報処理の研究経験者が多く活躍する当社では現在ソフトウェアリサーチャー(研究職)を採用中
- ◆情報処理の研究で培った深層学習、画像処理等の経験を、先端ソフトウェア研究開発で発揮しませんか
- 当社エンジニアの5割が博士号取得者、8割が博士課程出身

活かせる力 博士課程での研究で培った課題追究力、論理的思考力、実用的な数学の経験(統計、シミュレーション、データ解析等)を重視。プログラミング技術は研修等で習得できます。

業務内容 最先端ソフトウェアの研究開発
人工知能、機械学習・ディープラーニング、データサイエンス、画像処理、検査・計測・ロボット、自然言語処理、ヒューマンインタフェース、組込み制御などの新アルゴリズム研究開発。

採用条件 ライフワークとして、研究開発への意欲が強い方
・博士号の取得、博士課程での専攻分野はいずれも不問。
・博士後期課程修了/中退見込、あるいは修了/中退後5年程度以内の方。
・プログラミング未経験者でも、これから技術を習得して、先端ソフトウェア研究開発業務で幅広く社会貢献を行いたい方。
・日本語でのドキュメント作成や打ち合わせなどが可能なネイティブレベルの日本語力をお持ちの方。

募集期間 随時
勤務地 希望考慮(原則住居の移動を伴う転勤なし)

・当社ラボ/京都本社・京阪奈・名古屋・横浜・東京・筑波
・当社ラボ周辺の客先プロジェクト所在地

応募方法 当社HPの応募フォームよりご応募下さい。
連絡先 管理企画センター人事部 吉田・福原・岩前、e-mail: saiyou@tome.jp



面白い事をやって社会や生活を変える

EIC 電子情報通信学会発行図書案内

会議・プレゼンテーションのバリアフリー
——“だれでも参加”を目指す実践マニュアル——



電子情報通信学会
情報保障ワーキンググループ

A5判 ソフトカバー
定価(本体1,900円+税)

人に優しいイベントや、
分かりやすい発表の手引に!

本会発行単行本の内容に関する詳細は
下記Webページを御参照下さい。
<https://www.ieice.org/jpn/books/tankmokuoku.html>

信学会 目録 で検索!

電子情報通信学会 会員サービス部 会員課
TEL: 03-3433-6691(代)
kaiin@ieice.org

☆☆☆ 好評発売中! ☆☆☆

伝送理論の基礎と 光ファイバ通信への応用

笠 史郎 著

A5判 ソフトカバー
定価(本体3,800円+税)

伝送・通信理論、光ファイバ通信が
この1冊で全て分かる

話し言葉対話の計算モデル

島津 明 中野幹生 共著
堂坂浩二 川森雅仁

A5判 ソフトカバー
定価(本体3,400円+税)

話し言葉対話を扱うための基礎

「相互協力に関する覚書」に基づき、割引価格(2割引)で御購入頂けます。

4



PREFACE

巻頭コラム

184 誰一人取り残さないために情報技術が果たす役割 浅川智恵子

SPECIAL FEATURES

特集

面白いぞ量子技術

186 編集にあたって 袖美樹子

188 概要

お知らせ

特集記事はオンラインのみの掲載となります（本誌には「編集にあたって」「概要」のみ掲載されます）。オンライン記事（電子図書館）の閲覧方法につきましては本誌 210 ページに掲載しておりますのでご確認くださいませよう願いたします。

教育コーナー：ぺた語義

191 ■ 教育の ICT 化を推進するためには 前田健太朗

連載：情報の授業をしよう！

192 ■ 入試問題でテキストマイニング 中山享司

199 連載：★先生、質問です！

連載：★ビブリオ・トークー私のオススメー

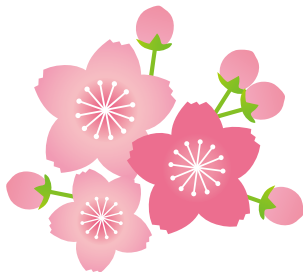
200 日本語から記号論理へ 小林真也

連載：★5分で分かる!? 有名論文ナメ読み

202 Listen, Attend and Spell: A Neural Network for Large Vocabulary Conversational Speech Recognition 増村 亮

会議レポート

204 VLDB 2020 開催報告 石川佳治



《記号の説明》

■ 基礎 ■ 専門家向け
■ 応用 ■ 一般（非専門家）向け ★ Jr. ジュニア会員向け
※各記事に指標がついていますので参考にさせていただきます

情報処理

常時更新中!

「情報処理」オンライン版 目次

https://www.ipsj.or.jp/magazine/contents_m_e.html

※オンラインでのみ掲載している記事の目次を掲載しております (目次から電子図書館の各記事へリンクしております)。



■ Vol.62 No.4

特集：面白いぞ量子技術

- e1 ■ 1. 量子コンピュータのあけぼの—今そこにある量子コンピュータに触れよう (今井 浩)
- e8 ■ 2. 量子アニーリングは死んだのか—研究の現状から思うこと— (大関真之)
- e15 ■ 3. 量子技術を利用した次世代アクセラレータの活用 (多和田雅師・田中 宗・松田佳希・楊 天任)
- e22 ■ 4. 量子コンピュータを用いた金融計算 (宇野隼平)
- e28 ■ 5. 量子コンピュータと量子化学計算—量子コンピュータによって量子化学は恩恵を受けるのか?— (大西裕也)
- e35 ■ 6. 量子計算は機械学習に使えるか—近未来／誤り耐性量子計算のための量子アルゴリズム— (御手洗光祐)
- e41 ■ 7. ダイヤモンド量子センサの可能性—ピンクダイヤモンドが高感度なセンサに— (波多野睦子)
- e47 ■ 8. 量子暗号の原理と実用化に向けた動向—絶対安全な通信の実現に向けて— (水谷明博)
- e53 ■ 9. 量子コンピュータハッカソン—コミュニティによる量子人材育成— (小林有里・松尾惇士・沼田祈史)

解説

- e61 ■ 「情報教育課程の設計指針」解説 (萩谷昌己)

「情報処理」note

<https://note.com/ipsj>

※人気記事や最新記事のチラ見せ, 無料で読める記事などさまざまなコンテンツを公開していきます。



- | | |
|--|---------------------|
| 206 会員の広場 | 212 有料会告 |
| 208 論文誌ジャーナル掲載論文リスト／論文誌トランザクション掲載論文リスト／IPJSカレンダー | 213 有料会告について |
| 209 【重要】過去のプログラミング・シンポジウム報告集の利用許諾について | 217 英文目次／アンケート |
| 210 【ご案内】会誌「情報処理」のオンライン記事について | 218 編集室／次号予定目次 |
| 211 人材募集 | 219 掲載広告カタログ・資料請求用紙 |
| | 220 賛助会員のご紹介 |

■会誌編集委員会

編集長：稲見 昌彦
 副編集長：大山 恵弘・加藤 由花・中田真城子
 担当理事：清水 佳奈・井上 創造
 本号エディタ：
 五十嵐悠紀・江渡浩一郎・大石 康智・大川 徳之・太田 智美・
 岡本 雅子・折田 明子・角田 博保・桂井麻里衣・金子 格・
 川上 玲・河原 亮・楠 房子・櫻 惇志・須川 賢洋・
 袖 美樹子・高木 拓也・中島 一彰・西川 記史・坂東 宏和・
 細野 繁・堀井 洋・福地健太郎・坊農 真弓・水野加寿代・
 山本ゆうか・湯村 翼

理事からのメッセージ：

https://www.ipsj.or.jp/annai/aboutipsj/riji_message.html

■情報処理学会事務局本部

〒101-0062 東京都千代田区神田駿河台1-5 化学会館4F
 Tel(03)3518-8374 (代表) Fax(03)3518-8375
 E-mail: soumu@ipsj.or.jp <https://www.ipsj.or.jp/>
 郵便振替口座 00150-4-83484
 銀行振込 (いずれも普通預金口座)
 みずほ銀行虎ノ門支店 1013945
 三菱UFJ銀行本店 7636858
 名義人：一般社団法人 情報処理学会
 名義人カナ：シヤ) ジョウホウシヨリガツカイ

■規格部 情報規格調査会

〒105-0011 東京都港区芝公園3-5-8 機械振興会館308-3
 Tel(03)3431-2808 Fax(03)3431-6493
 E-mail: standards@itscj.ipsj.or.jp <https://www.itscj.ipsj.or.jp/>
 ■支 部 北海道／東北／東海／北陸／関西／中国／四国／九州

電子版
-DIGITAL VER-



Kindle



Fujisan



情報学広場



誰一人取り残さないために 情報技術が果たす役割

■ 浅川 智恵子



私の学生時代、視覚障がい者が新聞を読み、銀行通帳を確認するためには、ボランティアに点訳を依頼したり周囲の人に読み上げてもらう必要がありました。本当に大変な時代でした。そんな経験から1985年にIBMに入社してからは情報アクセシビリティの研究開発に取り組みました。ちょうど入社したころに市場に出てきたPCを活用して点字をデジタル化し、編集や共有を可能にするシステムを実用化しました。1990年代には世界初の実用的な音声ブラウザを開発し、世界中の視覚障がい者が簡単にWebへアクセスできるようにしたことは私の誇りです。そして2021年の現在、スマートフォンを使えばいつでもどこでも最新のニュースを読むことができ、オンラインバンキングを使えば銀行口座も簡単に確認できます。こうした革命的なアクセシビリティの向上は、PC、音声合成技術、Webそして携帯端末といった情報技術が成し遂げました。

デジタルデータのアクセシビリティは向上しました。しかし視覚障がい者は「身の回りの実世界」にはまだまだアクセスできていません。街中を歩いているときに周囲にどんなお店があるのか、どんな人が歩いているのか、10メートル先にどんな障害物があるのか、こうした情報を知ることはできません。さらにコロナ禍において新たな課題にも直面しています。横断歩道の押しボタンやエレベータのボタンを手で触って探すことへの不安や、正しい距離を保って列に並ぶことの難しさ、困ったときに街中で周囲の人に声をかけづら

■ 浅川 智恵子

IBM フェロー, IBM T.J.ワトソン研究所

1985年日本IBMに入社。以来アクセシビリティの研究に従事。2009年IBMフェロー就任。2013年紫綬褒章受章。現在カーネギーメロン大学の客員教授を兼務。2021年日本科学未来館館長に就任予定。工学博士。



くなったことなどさまざまな困難が報告されています。

そこで、2017年に立ち上げたのがAIスーツケースプロジェクトです。スーツケース型ロボットにカメラをはじめとしたさまざまなセンサを搭載し、AIと組み合わせることで、周囲の歩行者や障害物を回避して安全に目的地に到達できるだけでなく、行列を認識し、正しい距離をとって並ぶ機能なども実装しました。2019年11月には実際にショッピングモールの中で自由に移動できるバージョンが完成しました。現在テストを行っていますが、周囲の歩行者や障害物との衝突を気にすることなく自由にお店を選んでモールの中を歩くことはウィンドウショッピングに近いような新しい感覚です。コンピュータビジョンをはじめとしたAI技術を活用することでコンピュータが視覚障がい者の目として身の回りの実世界を認識してくれるようになる日が現実のものになろうとしています。

“Leaving No One Behind.” これはSDGsの基本理念です。「だれひとり取り残さない」というのは非常に高いハードルのように感じるかもしれませんが、しかし、一人ひとりの技術者が多様性を持ったユーザがいることを常に心に留めて開発を進めれば、確実に前進できるはずです。私も研究者と視覚障がい者ユーザという2つの立場をうまく融合させて、情報技術が実現する共生社会の形を示していきたいと思います。

面白いぞ量子技術

編集にあたって

袖美樹子 | 国際高等専門学校

2019年10月米Googleが科学誌Natureに量子コンピュータが、スーパーコンピュータでは処理に1万年を要する演算をたった200秒で行い、史上はじめて量子超越性を実証した、と発表した。量子超越性とは、スーパーコンピュータを始めとする現在の計算機ではとても長い時間かかる何らかの計算を、量子コンピュータが圧倒的に高速に実行できることを指す。量子コンピュータの新たな時代の幕開けである。

量子コンピュータが脚光をあびる背景には、現在これ以上の半導体微細化が困難で、ムーアの法則が限界を迎える一方で、より高性能なコンピュータのニーズがAI、創薬、暗号化等の分野において高まっているためと考えられる。実際に量子コンピュータは金融、製造、交通、化学、情報の分野で実用化にむけた試行が進んでいる。そこで本特集では量子技術の現状を紹介いただく。

第1の記事では、東京大学教授・本会量子ソフトウェア研究会主査である今井浩氏による「量子コンピュータのあけぼの—今そこにある量子コンピュータに触れよう」である。量子コンピュータとは何か？ 原理や従来のコンピュータとの違いは？ 何ができるのか？を初めて量子コンピュータについて学ぶ方にも理解いただけるよう分かりやすく解説をいただいた。

第2の記事は、東北大学・東京工業大学教授、(株)シグマアイ代表取締役である大関真之氏による「量子アニーリングは死んだのか—研究の現状から思うこと—」である。量子アニーリングとは、組合せ最適化問題を、物理現象に置き換え計算させることで、効率良く問題を解くために提唱された計算手法で、2011年に世界初の商用量子コンピュータを謳ったD-Wave Oneで採用された技術である。本記事では、量子アニーリング手法の量子コンピュータにおける意義、歴史的背景を解説いただく。

第3の記事は、早稲田大学多和田雅師氏、慶應義塾大学田中宗氏、(株)フィックスターズ松田佳希氏、(株)QunaSys楊天任氏による「量子技術を利用した次世代アクセラレータの活用」である。量子コンピュータは量子力学を計算原理に使っている度合いで代表的なものを並べると誤り耐性量子コンピュータ、NISQ量子コンピュータ、量子シミュレータ、量子アニーリングマシン、イジングマシンとなる。本記事ではイジングマシン、誤り耐性量子コンピュータ、NISQ量子コンピュータについて活用事例を含め解説いただく。

第4の記事は、(株)みずほ情報総研宇野隼平氏による「量子コンピュータを用いた金融計算」である。金融分野においては、AIを利用して投資や運用の支援をするロボアドバイザー、コンピュータを用いて自動的に取引を行うアルゴリズム取引、ブロックチェーン技術による仮想通貨など顧客情報や取引データ等の大量の情報を高速に処理する必要がある業務が山積している。本記事では、金融機関における量子コンピュータ活用に向けた取り組みのうち、特にデリバティブ(金融派生商品)の価格評価を中心に解説いただく。

第5の記事は、(株)JSR大西裕也氏による「量子コンピュータと量子化学計算—量子コンピュータによって量子化学は恩恵を受けるのか?—」である。量子コンピュータの活用先の1つとして有望視されているのが分子レベルのミクロな現象を「シミュレーション」することができる量子化学計算である。量子化学計算はアカデミックのみならず製薬企業から石油産業や素材産業まで、すでに多くの場面で産業的にも活用されている。また、機械学習を用いて材料の性能予測や構造提案を行うマテリアルズ・インフォマティクスと呼ばれる手法のためのデータ作成にも使われている。本記事では、量子

化学計算を従来のコンピュータで扱うことの難しさ、量子コンピュータでの計算可能性に関して解説いただく。

第6の記事は、大阪大学、(株) Qunasyys 最高戦略責任者である御手洗光祐氏による「量子計算は機械学習に使えるか—近未来/誤り耐性量子計算のための量子アルゴリズム—」である。近年量子コンピュータによる機械学習を高速化するためのアルゴリズム開発が盛んになってきた。これらのアルゴリズムは量子機械学習アルゴリズムと呼ばれている。本記事では量子機械学習アルゴリズムについてその概要を解説いただく。特に、近年の研究動向を踏まえ、現在何ができるかを解説いただく。また今後の展望についても解説いただく。

第7の記事は、東京工業大学教授波多野睦子氏による「ダイヤモンド量子センサの可能性—ピンクダイヤモンドが高感度なセンサに—」である。ダイヤモンド量子センサは、量子力学的効果を利用して感度や分解能を物理法則の極限まで高められる次世代センサとして注目されている。ダイヤモンド量子センサはベクトル磁場計測により、神経ネットワーク内の信号の発生と伝播の方向性、外部刺激に対する脳内反応の経路が解析できるようになり、脳内、特に脳深部の神経電流の分布を推定する精度が向上することが期待されている。脳や神経などの生体計測技術の革新は、ヘルスケア、脳疾患の予防や治療などの医療、さらには脳型情報処理などの応用に繋がると考えられている。本記事では、ダイヤモンド量子センサの可能性を中心に、その原理、人工的に作製する技術、量子プロトコルを用いた計測、および応用を解説いただく。

第8の記事は、三菱電機(株) 水谷明博氏による「量子暗号の原理と実用化に向けた動向—絶対安全な通信の実現に向けて—」である。量子暗号とは物理学の

分野の1つである、量子力学の理論をもとにした暗号技術で盗聴を完全に防ぐことができる暗号技術として期待されている。量子力学では、未知の量子状態を測定して状態を知ることができず(不確定性原理)、未知の量子状態のコピーを作ることできない(量子複製不可能定理)ため、盗聴をすることができない。量子もつれと呼ばれる量子力学的な非局所相関の性質から、無条件安全性が保障される。本稿では、現代暗号との違い、量子暗号の原理を解説いただく。

第9の記事では、IBM Research - Tokyo 小林有里氏、松尾惇士氏、沼田祈史氏による「量子コンピュータハッカソン—コミュニティによる量子人材育成—」である。IBMは2016年世界で初めてクラウド型量子コンピュータを無償公開するなど、量子コンピュータの分野で常に先頭を歩んでいる企業である。現在、量子計算を可能とするIBMの量子ソフトウェア開発キット Qiskit のユーザは28万人を超えている。本特集では、量子人材育成を目標とした量子コンピュータハッカソンを紹介いただく。

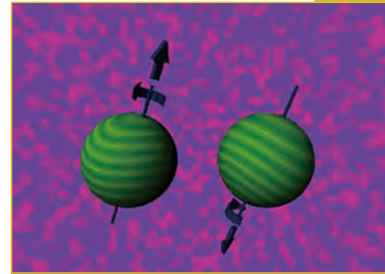
量子技術は、経済・社会等を飛躍的・非連続的に発展させる鍵となるコア技術であり、生産性革命の実現、安全・安心の確保、健康・長寿社会の実現に欠かせない技術であると言われている。そのため、日本では戦略的な取り組みが行われており、主要技術領域として①量子コンピュータ・量子シミュレーション②量子計測・センシング③量子通信・暗号④量子マテリアル(量子物性・材料)が定められている。本特集では、これらの一部を解説いただいた。本会としては量子ソフトウェア研究会を運営するなど尽力している分野である。今後の量子技術の飛躍的進歩(quantum leap)に期待したい。

(2021年2月9日)

1 量子コンピュータのあけぼの —今そこにある量子コンピュータに触れよう

今井 浩 | 東京大学

量子コンピュータというキーワードを情報処理分野で頻繁に聞くようになった。本会でも 2020 年度より量子ソフトウェア研究会が立ち上がり、学会として量子コンピュータをもつばら扱う研究会も活動を開始している。「量子」と聞くと、従来の情報科学・情報工学の専門課程で特段に量子力学を履修しているわけでもなく、一瞬それ物理でしょ、電子工学でしょ、という違う分野のものといった発想がよぎったりするのかもしれない。本稿では、量子ソフトウェア研究会発足に示されるように、ぜひ読者の方に量子コンピュータが到来する未来を紹介したい。



応
般

2 量子アニーリングは死んだのか —研究の現状から思うこと—

大関真之 | 東北大学/東京工業大学/(株)シグマアイ

2019 年秋頃に発表された量子超越性。それ以来量子コンピュータに対して強い期待が寄せられている。ご存知だろうか。世界初の商用量子コンピュータとして登場した D-Wave Systems 社の量子アニーリングマシンを。組合せ最適化問題を解くために特化した量子デバイスであり、本道の量子コンピュータとはまったく違う様相を示す。次第に量子コンピュータに対する熱が高まる中、ひっそりとしてきた量子アニーリングについて、その現状を振り返り、期待される今後の研究の方向性を紹介する。

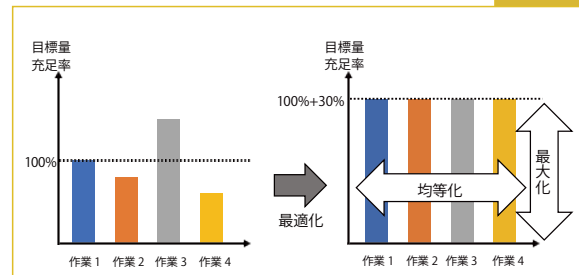
基
専

3 量子技術を利用した次世代アクセラレータの活用

多和田雅師 | 早稲田大学 田中 宗 | 慶應義塾大学

松田佳希 | (株)フィックスターズ 楊 天任 | (株)QunaSys

次世代アクセラレータと呼ばれる量子技術や古典技術を用いた新原理の計算機が期待されている。これら次世代アクセラレータは種類ごとに使用方法が異なり、計算分野の得意不得意が存在する。使用には専門知識が必要でありコストが高いため、各アクセラレータ固有の使用法や性質を考慮し、プログラムの部分ごとに適切に割り当てるソフトウェアが要望されている。本稿では、次世代アクセラレータの種類と活用事例、および適切にアクセラレータを使用するソフトウェアとその要素技術の研究動向を紹介する。



応
般

4 量子コンピュータを用いた金融計算

応
般

宇野隼平 | みずほ情報総研 (株)

金融業界では、将来的な計算量の増大に備え、量子コンピュータの応用先の検討を開始している。ここでは、金融分野への応用先として期待されているシミュレーション、機械学習、最適化のうち、特にシミュレーションを使ったデリバティブ価格評価について、筆者らの最近の取り組みを含めて紹介する。

シミュレーション

- ✓ デリバティブ価格評価
- ✓ 保有資産のリスク評価

機械学習

- ✓ 株価・金融危機予測
- ✓ 信用リスク評価
- ✓ 不正検知

最適化

- ✓ ポートフォリオ最適化
- ✓ 裁定取引
- ✓ パッシブ運用

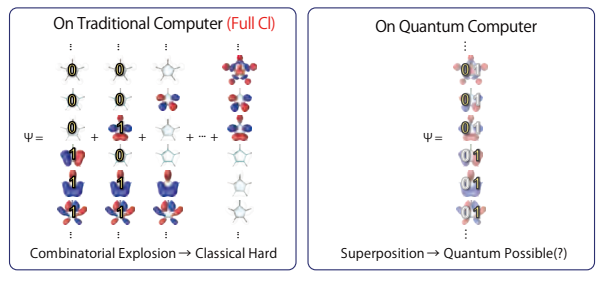
5 量子コンピュータと量子化学計算

—量子コンピュータによって量子化学は恩恵を受けるのか?—

応
般

大西裕也 | JSR (株) RD テクノロジー・デジタル変革センター マテリアルズ・インフォマティクス推進室

2010年代後半から再び盛り上がりを見せている量子コンピュータの応用先として、量子化学計算が注目されている。本稿では量子化学計算とは何か、そして量子コンピュータによってどのような恩恵が量子化学計算にもたらされるのかを概観し、その道のりは決して平坦ではないが、制御レベル、ミドルウェア、ソフトウェア、アルゴリズムの面では非常に興味深い挑戦がいくつもあることを述べる。



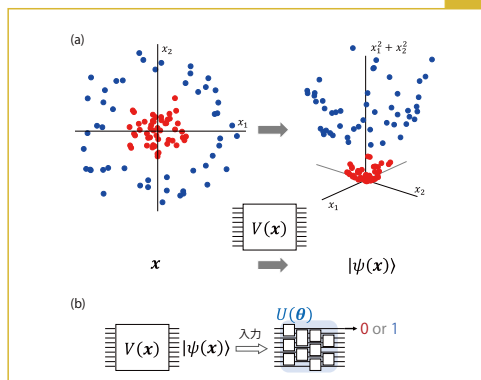
6 量子計算は機械学習に使えるか

—近未来/誤り耐性量子計算のための量子アルゴリズム—

応
般

御手洗光祐 | 大阪大学大学院基礎工学研究科

量子コンピュータハードウェアの発展に相まって、近年量子コンピュータへの期待が高まっている。本稿では、量子コンピュータの基礎的な原理も交えながら、量子コンピュータを用いた機械学習手法について最近の研究を概観する。計算中のエラーが無視できない近未来の量子コンピュータに向けたものと、量子誤り訂正によってそのようなエラーが無視できる将来の量子コンピュータに向けたものの2つに大別して解説する。

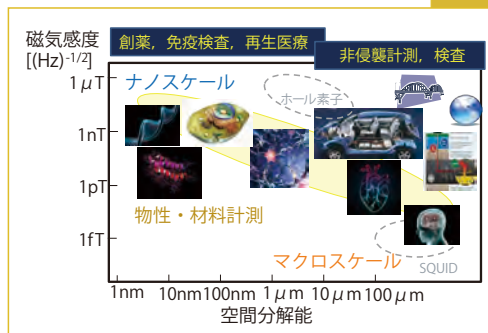


7 ダイヤモンド量子センサの可能性 —ピンクダイヤモンドが高感度なセンサに—

応
般

波多野睦子 | 東京工業大学工学院

ダイヤモンド量子センサは、原子レベルのナノスケール構造、常温大気中で動作、磁場・温度の同時計測が可能、CVDや電子線照射等の半導体技術で製造可能、等の特徴を有する。生体親和性を活かした、脳磁等の生体計測と、耐環境性・広い動作範囲を活かしたエネルギーデバイスモニタリングが重要な応用であり、安全安心社会、低炭素社会に貢献するものである。その計測精度の向上と、応用の発展には本会との連携が必要である。

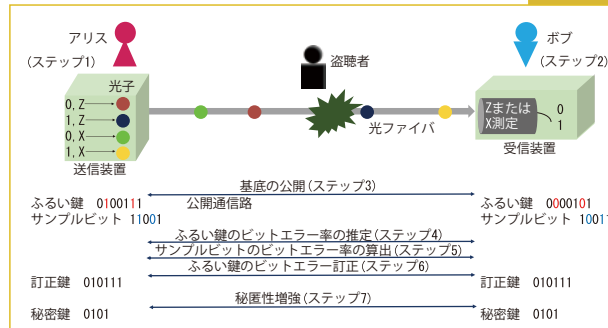


8 量子暗号の原理と実用化に向けた動向 —絶対安全な通信の実現に向けて—

応
般

水谷明博 | 三菱電機 (株) 情報技術総合研究所

量子暗号は物理法則によって安全性が担保された鍵を2者に配送する技術である。この鍵を用いてワンタイムパッドで平文を暗号化することで、無限の計算能力を持つ盗聴者に対しても安全な暗号通信が実現できる。本稿では、はじめに普段我々が使っている暗号と量子暗号の比較を行う。次に量子暗号の前提をまとめた後、代表的な量子暗号プロトコルを説明し、安全性の原理を概説する。最後に、量子暗号の最近の開発動向について述べる。



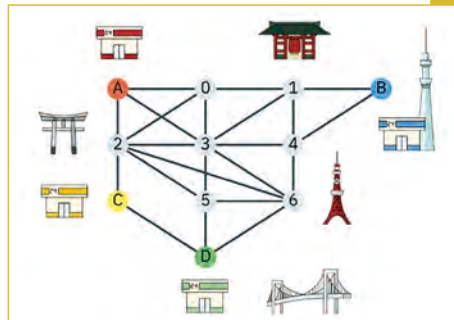
9 量子コンピュータハッカソン —コミュニティによる量子人材育成—

応
般

Jr.

小林有里・松尾惇士・沼田祈史 | IBM Research - Tokyo

量子コンピューティングとその技術が注目を集める中、量子研究や量子情報科学の分野で活躍できる人材の重要性が一段と高まっている。本稿では近年、世界から数千人規模が集い知識とスキルの研鑽の場となっているIBMの量子コンピュータハッカソン「IBM Quantum Challenge」に注目し、量子人材育成の観点からハッカソンが持つ教育的価値の可能性を考察する。



[面白いぞ量子技術]

1 量子コンピュータのあけぼの

—今そこにある量子コンピュータに触れよう

基
般

今井 浩 | 東京大学

量子コンピュータ

コンピュータは大まかにはハードウェアとソフトウェアからなっている。量子コンピュータは、

- ハードウェアが量子力学原理で動作し、
- ソフトウェアが量子力学制御の操作を行う

ものである。今のコンピュータは量子力学以前の力学である古典力学（ニュートン力学に代表される）で動作している。量子力学は古典力学より優れた点を持つが、量子力学に従って制御することなど、現在でもまだ完全に行うのは難しい。でも量子コンピュータならもっといいことができるのでは、という構想が1980年頃に複数示された。

1つは数学者のManinによるもので、1980年に出版された『計算可能性と計算不可能性』という本の第1章最後の3段落^{☆1}でその構想を語っている。これに触発されたKitaevは、1982年には量子計算の研究を開始し1990年代半ばに量子位相推定アルゴリズムやトポロジカル量子計算等で量子計算基礎で大きな貢献をしている^{☆2}。

今よく知られている構想の1つは、1981年のThe Physics of Computation^{☆3}というMIT Laboratory for Computer Science (LCS) とIBMが組

織^{☆4}した会議で、Feynmanが行ったSimulation of Physicsという基調講演²⁾である。その中で、Feynmanは量子力学をコンピュータでシミュレーションすることは、従来コンピュータでは計算困難であるが、量子コンピュータであれば高速に行えるのではという考えを示している。

これらの共通することは、

量子コンピュータは、従来コンピュータのコンピュータでは計算困難な問題を、効率良く解くことができるだろう

という思い・研究プログラムである。根拠なく主張しているわけではなく、そのための基礎的課題の検討を行った上で研究コミュニティに刺激を与えている。その他の構想も含め、この時期が量子コンピュータの力が従来コンピュータのそれを凌駕する可能性が認識され、構想から量子コンピュータの研究へと展開するあけぼのとなっている。

本稿では、この展開以降の段階的変革をとげるあけぼのについて見ていきたい。

☆1 Manin¹⁾のAppendixにKitaevによる訳がある。

☆2 KitaevのMacArthur Fellow受賞ニュース, IEEE Spectrum, 2008.

☆3 MIT Endicott Houseの会議ページ

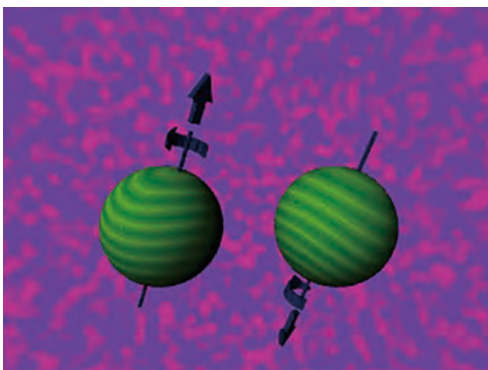
☆4 MIT LCSの前身組織の所長だったFredkinと研究員のToffoli(それぞれの名前を冠した可逆ゲートあり)とIBM研究所で非可逆回路でのエントロピー消失と熱発生原理などの研究を行っていたLandauerによる。

1 量子ビット計算で初めてできること

量子コンピュータの力を調べる方向性が示されて、次に実際にその力を示す研究が出てきた。ここで基礎をおさえておこう。従来コンピュータは0か1かを表す1ビットを基本とする。量子コンピュータでは、それが1量子ビットとなる。1量子ビットのイメージを図-1に示す。この図は一見地球が変な空間に浮かんでいるようにも見え、自転軸も傾いている。地球の場合、右手系で北極の方向のスピンのようになっており、それで0を表し、逆に南極方向のスピンの1を表す。スピンなので、実は球面分の自由度を持っており、まずはそのどの方向でも持てるとする（実際にはここを離散化）。

このような1量子ビットだけで簡単な量子計算する量子暗号方式に触れよう。Bennett, Brassardは1984年の国際会議での招待論文の中で、現在BB84と呼ばれる量子鍵配送方式を提案した。Shannonの完全秘匿性に関する定理から、平文と同じ長さのランダムな秘密鍵を2者間で共有できると、情報理論的に安全という究極の基準での安全性を実現できる。従来計算・通信のレベルではその高いレベルを有する暗号方式はなく、BB84は量子力学での不確定性原理を用いて初めて達成したものである。

量子計算としては、1量子ビットを回転（ユニタリ変換）し、標準的な測定を行うだけである。実現にあたっては、1量子ビットを伝送する1光子



■ 図-1 2つのスピン：左側は右手系で上向きで0を、右側は下向きで1を表現。|01⟩と表される。

（1粒子の光；光は量子力学では波でもあり粒子でもある）が理想であるが、その生成がまだ難しいので、現在の量子暗号システムでは弱いレーザー光を用い、ソフトウェアとして光強度をデコイ（おとり）とし、統計処理することで、セキュリティ要求に応じた安全性を保証するものが開発されている。日本でもこの量子暗号が事業化されていることは、種々CMを通じてご存知と思う^{☆5}。

ここで量子力学の概念が出てきて壁を感じる方もいるかもしれないが、その壁は量子コンピュータ自体を使うことで乗り越えられるのだというのを見ていこう。

量子計算を線形代数・プログラムで理解する

量子力学の理解は、きちんと深く量子計算を極めるには必要であろう^{☆6}。一方で、大学学部の量子力学講義（2, 3学期にわたる）ものを知っていないと、量子計算が理解できないわけではない。基本、大学入門数学での線形代数が理解できていれば取り組むことができる。

量子暗号BB84を自分で送信者・受信者を演じて、今利用可能な量子コンピュータのクラウドサービスを使って実現してみよう。量子ビットで0, 1を表現するのに2次元ベクトルを使って

$$0 \mapsto |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad 1 \mapsto |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

と表現し^{☆7}、必要な操作は 2×2 行列で

☆5 このように、量子コンピュータ構想が示された1980年代初めのあけぼのから、すぐに情報セキュリティの核となる量子暗号方式が提案され、その後息の長い研究開発を通して社会実装に至っている、というすごさも理解していただけるとありがたい。

☆6 さらに無限次元の場合で関数解析とかも分かっているとためになるし、トポロジカル量子計算ではトポロジーの基礎も分かっていた方がよい。

☆7 量子力学のDiracのket記法の $|0\rangle, |1\rangle$ を初めて見た人は、単に縦ベクトルで、0, 1を表現するものと理解を。

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

などを使って、Python 流に操作の中核部分を書いて

```
qc = QuantumCircuit(q, c)
qc.h(q)
qc.measure(q, c)
qc.draw()
```

とすると、初期はデフォルト 0 が符号化されてたところを、

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

となり、量子力学の最も基本的な測定法では、測定結果は 0, 1 を等確率で得ることになる^{☆8}。すなわち、初期状態に関する情報は何も得られなくなっていて、量子不確定性がこの小さな事例で発現している。一方、`qc.h(q)`を`qc.X(q)`で取り替えると、

$$X|0\rangle = |1\rangle \quad (\text{同様に } X|1\rangle = |0\rangle)$$

出力は必ず 1 となり、初期値 0 の否定を計算したことになる (X は NOT 操作)。

1 量子ビット演算として H に加えシフト行列 S と T ゲート T を用い、2 量子ビット演算で制御 NOT という 4×4 の行列を量子計算を実行する量子回路の基本ゲートとすると、これらを繰り返し適用していくことによって、 n 量子ビットに掛ける任意の $2^n \times 2^n$ のユニタリ行列を指定精度内で近似することができる^{☆9}。図-1に加え、6 量子ビットのスピンを図-2に示す。

すると、量子計算は n 個の 0 を表す n 量子ビットを初期状態に、所望の結果を得られる量子回路で計算し、最後に測定することで出力を得ることともいえる。ハードウェアで、これら基本ゲートを実現

☆8 こういうのが量子力学の不可思議なところ。

☆9 量子力学では 1 量子ビット 2 つを合成して、1 つの 2 量子ビットにすることは、テンソル積 (Kronecker 積) をとることに対応する。

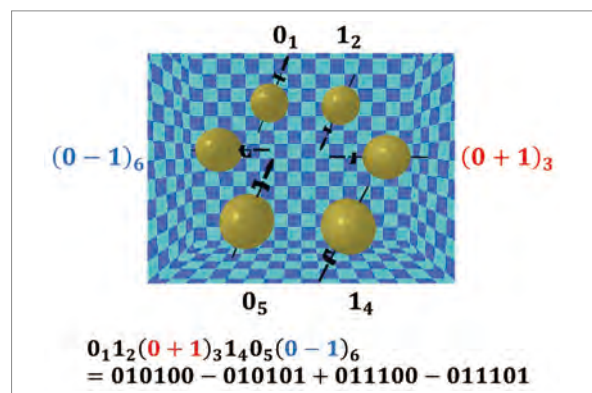
する操作を行えると、量子力学の世界では 2^n 次元の演算が基本ゲートの適用回数の時間で計算でき、測定をすれば所望の n ビットの出力を得ることができるのが、量子コンピュータが従来のコンピュータを凌駕し得るだろうと信じたくなる理由である。

量子計算だからできること

1 量子ビットでの量子計算・量子情報処理では、1980 年代に醸成された量子暗号の研究が始まり、現在では事業化も通して社会に浸透するレベルになっている。しかし、実際にはその過程で停滞もあった。日本の場合、2000 年頃からの NICT や JST のプロジェクトを通して現状まで突破してきたところであるが、BB84 の原論文が当初国際会議で評価されず、招待論文の機会に発表されていることなど、新奇分野・原理であるがゆえの評価されにくい時期もあった。

そういう停滞時期を打破したのは、量子計算だからこそ初めて可能になることを社会的インパクトが大きい問題で示した 1994 年の Shor³⁾ の量子多項式時間の素因数分解アルゴリズムである。このブレークスルーをもたらしたアルゴリズムは次の 2 点で卓越している。

(a) 1978 年提案の RSA 公開鍵暗号系は、インター



■図-2 6つのスピン水平向きのスピンは各々 0, 1 を半々の違う重み (振幅) で合成した状態。これは単純な状態で、後述の量子エンタングルメントがあると、このような表現はできない意。

ネットでの基盤技術となっているところを、その安全性を素因数分解の計算困難さにおいていた。Shor のアルゴリズムは、ひとたび量子コンピュータが大規模問題を解けることになると、RSA 暗号の安全性が崩壊してしまうことを意味し、社会インパクトが大きい。

(b) 量子計算のアルゴリズム論の観点で、非常に巧妙に構築されており、そこから一連の量子計算で効率良く解く枠組みを提供したこと。

(a) については、過大に思われる方もいるかもしれないが、共通鍵暗号の世界標準 AES などを制定している NIST が、2016 年から大規模量子コンピュータが存在しても安全な公開鍵暗号を選定するプロジェクトを進めている。インターネットのセキュリティは社会インフラで、それを更新するには十分な余裕期間が必要という考えもあるかもしれない^{☆10}。

(b) については、Shor のアルゴリズムのポイントは 2^n 次元の離散フーリエ変換を使うという点だけではないことである。確かに、量子コンピュータで $O(n^3)$ で計算できるという先行研究をうまく使った部分は重要で、それは Shor のアルゴリズムの後半部分であって、前半部分では位数発見問題という周期関数の周期を求める問題への変換が行われているところも重要な貢献であることを紹介しておく。量子計算を量子回路でのゲートセットを限定して部分クラスを考える理論から、前半部の巧妙さが鍵となっていることも示唆されている。また、Shor の位数発見問題への変換は、Miller の 1976 年の素因数分解の従来の計算量に関する論文での 1 つの成果であることも指摘しておきたい。すなわち、量子アルゴリズムというのは、量子計算で新しいものを考えることだけではなく、従来の計算方式でのアルゴリズムをベースにして量子の風味を加えて劇的な高速化を実現することができる典型例となっている。

☆10 一方で、現時点ですぐに危惧を持つ必要はないことは、IPA の情報発信にもある。

Shor のアルゴリズムは (a) のような社会的インパクトも与えている一方、2 つの大きな未解決課題を提示している。

- 従来コンピュータでは、スパコンをもってしても素因数分解は計算困難である、ということが妥当だと思われてきたが、将来もしかして天才が従来コンピュータで高速に素因数分解を実行できることを示す可能性はゼロではない^{☆11}。
- 量子コンピュータで Shor のアルゴリズムを RSA 暗号破りに適用する場合、数百万量子ビットの誤り訂正可能な量子コンピュータ実現が必要で、それはまだ先であると思われており、かなりの課題を解決していかないとはいけなと予想されている。

Shor のアルゴリズムは、量子アルゴリズムで社会に影響を与えた最初のものであり、その拡張の Kitaev の位相推定アルゴリズムも含め、今後とも量子アルゴリズム研究での核をなすことは確かである。

量子計算だからできること 2

量子力学は、それ以前の力学（古典力学）での常識と合わない新奇性がある。量子力学の理論構築時に、本当にその理論が正しいのか、自然の摂理を表しているのかについて、議論がなされていた。たとえば、Physical Review の 1935 年の論文では、Einstein, Podolsky, Rosen によるその新奇性に関しての量子力学批判の論文（EPR 論文と呼ばれる）が 5 月に掲載されたのち、10 月には Bohr による反論を記述した論文が計算されるなど^{☆12}。

実はこれは最初に述べた、量子コンピュータ vs. 従来コンピュータの図式でも同様であり、上記では

☆11 量子アルゴリズム周辺で、従来方式では効率良く解けないと仮定していたのに、実際にはすぐにその仮定が間違っていたことが示された事例が結構ある。素因数分解問題の研究はもう半世紀近く行われてまだ見つけられてないので、そうたやすく解けないと思われているもの。

☆12 ちなみに両論文は同じタイトルである：Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

特集 Special Feature

Shor のアルゴリズムがこの図式で量子側でのブレークスルーをもたらしたものであることを述べた。前段落での量子力学理論に関する論争点も、実はこの計算での図式に発展させることができ、2020年1月に大きな成果が出ているので紹介しよう。

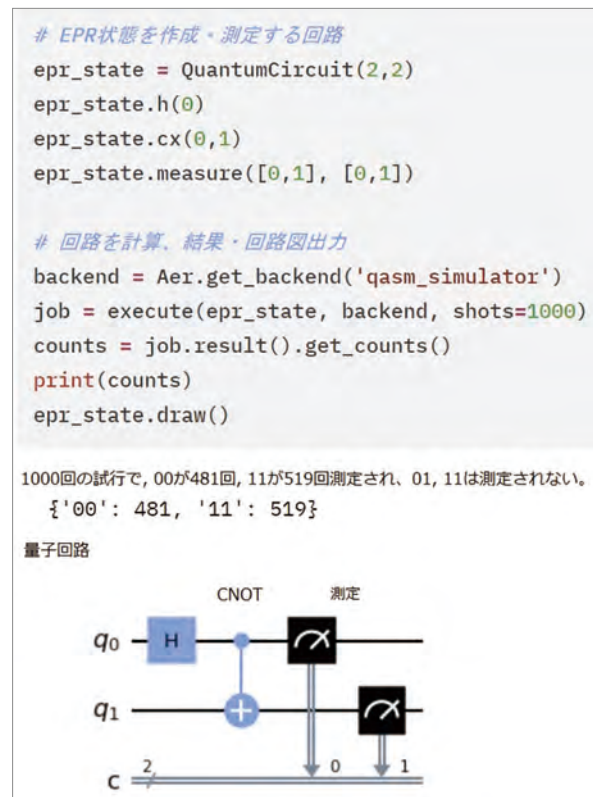
EPR論文の指摘は、現在量子エンタングルメント（あるいは量子もつれ）^{☆13}と呼ばれる概念が引き起こす不思議について論じている。それが不思議ではなく、実際に量子力学が成立しているのだと示すために、Bellは不等式に着目した。この不等式は古典確率では必ず成り立つ相関確率に関するもので、量子力学実験から量子エンタングルメントを通じて得られる量子測定確率ではその不等式が破れてしまうことを理論として示したものである。Bellの示した不等式は、ある意味皆がよく知っているもので、三角形で成り立つ三角不等式と対応している。誤解をおそれずイメージでいえば、量子エンタングルメントしている量子状態からの量子測定確率で対応する三角形を書くと、三角不等式が成立していないという不思議なことになる。ここでは、IBM Quantum Experienceを用いて、2量子ビットで量子エンタングルメントした状態（EPR状態）を計算・測定するプログラム例を図-3に示している。

量子力学実験の観点では、三角形では実験が困難ということで、三角不等式を拡張したCHSH不等式というものが、通常の教科書で単にBell不等式として紹介されている。そして、1982年にはAspectらのグループが光学実験で量子効果でCHSH不等式の破れる結果を得ている。

CHSH不等式は、情報科学のグラフと最適化の理論の言葉を使うと、完全2部グラフ $K_{2,2}$ に対する相関多面体の満たす不等式である。より一般の2部グラフをベースとして拡張した枠組みでの一般化Bell不等式を構成することができる。この拡張は、計算

量理論の分野でのランドマークとなる結果である1986年のGoldwasserらによる多証明者対話証明の理論とまさしく対応することが分かっている。2証明者対話証明のゲームの値が古典確率の上限に対応し、それを2証明者の間に量子エンタングルメントがある場合の対話証明ゲームの値がその上限を超えることがBell不等式の破れに対応する図-4。

この拡張のもと、EinsteinらのEPR論文が指摘した量子エンタングルメントの不思議は、量子力学の表現空間は線形代数が表す有限次元の空間を超え、無限次元空間も考えて関数解析の対象となることも関係している。2証明者の量子エンタングルメントの度合いが限られる場合は、計算量理論でNEXPという量子エンタングルメントがない場合のクラスと同等のことが示されていたが、Ito, Vidick⁴⁾が量子エンタングルメントが少なくとも量子計算のバ



■図-3 Qiskitでのプログラムのシミュレータでの計算例。2量子ビットのEPR状態というエンタングルしたものを測定すると、00, 11のみ測定され、EPRの指摘した不思議なことが起こっている。

☆13 複数量子ビットがエンタングルしていると、各量子ビットを図-1に示したようなスピンで表現できなくなっており、量子力学で独特な複雑な構造になっている。

ワーを真に増進する方向で有効であるという大きな結果を 2012 年に示した。それ以来、2 証明者間の量子エンタングルメントの量の上界を与えない一般の場合の解析が先端研究での目標になっていたが、次第に計算不可能なクラスまで難しくなるのではと研究者が予想しはじめ、ついに 2020 年に対話証明のゲームの値の計算が計算不可能になってしまうことが示された⁵⁾。より具体的には、そのゲームの値が計算できると、Turing マシンの停止問題という計算不可能な問題が解けることになるというものである。1936 年に Turing による計算の定義が Turing マシンの有限時間停止性によって与えられて以来、それが計算の定義として 100 年近く認められてきており、量子計算の観点からその定義を再考することもできるかもしれない。

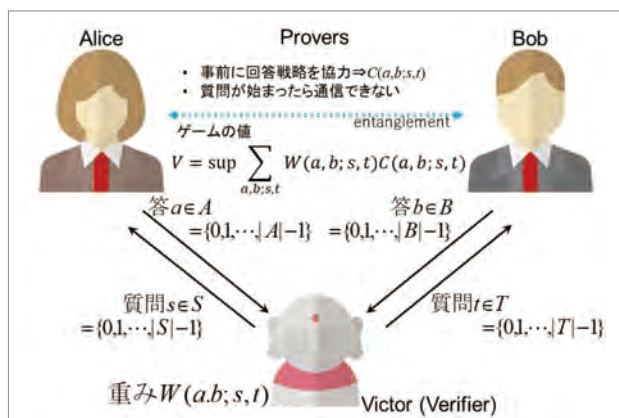
量子コンピュータシステムのあけぼの

本会に量子ソフトウェア研究会が設置された 1 つの原動力は、もっと将来のことと研究者の中で思われていたかもしれない量子コンピュータシステムの実現スピードが上がり、数十量子ビットのデバイスも出てきて、それを制御するソフトウェアも構築され、いよいよ皆が量子コンピュータを使える時代が来た点にある。2, 3 年後に 1,000 量子ビットを超

えるロードマップも示されたりしている。その点、本章のタイトルのように、ユーザが実際に使える量子コンピュータシステムと呼べるものがまさしく到来したというのである。一方、すでに来たのであれば、あけぼのの時期は超えつつあると思われるかもしれない。しかし、上記でできて広くユーザに供されているのは、まだまだ発展段階初期の量子コンピュータである。量子力学で Schrödinger 方程式に代表される連続量の世界の影響を受けたアナログ性もまだ有することや、量子状態が脆いことによるデコヒーレンスエラー、ゲート操作のエラー、測定エラーなどによる限界^{☆14}がある。

それら限界を乗り越えていくという観点からは、まさしく近未来量子コンピュータを大規模化・誤り訂正可能化・耐故障性保証する前のあけぼのの状態である。このような量子コンピュータシステムのあけぼの・曙光がやうやう差し込んできたところで、それを確とした陽光にしていく時期である。たとえば、本稿の第 1 章の書き出しで量子コンピュータのハードウェアとソフトウェアの記述が、従来コンピュータのきれいにレイヤ化された世界と違うなどといった違和感を持たれた方は、今このタイミングが最も面白い研究開発段階であることに思い至る可能性が高い。このような時期というのは、まさしく半世紀以上前に今のコンピュータの原型が発明されて動作し始めた黎明期に匹敵するもので、ぜひ多数の方が参画して未来を拓いていただけることを望むところである。

一般のユーザ向けに、量子コンピュータのクラウドサービスが提供されている。2016 年に開始された IBM Quantum Experience がさきがけで、そ



■ 図-4 一般化 Bell 不等式に対応する 2 証明者対話証明ゲーム：おおよざには、情報交換できない 2 名の家庭教師に個別にうまく質問する学生は、1 名の家庭教師に学ぶ場合より学習能力が大きくなる図式。

☆14 ちなみにこのような限界を書くと、現時点の量子コンピュータシステムは有用なのかという疑問がわいてくるかもしれないが、このレベルの量子コンピュータで効率良く解ける問題というのが多様に開拓されつつあることを念のため書いておきたい。代表例は、本稿で述べた Shor の位数発見アルゴリズムを拡張した Kitaev の位相推定の部分を、量子コンピュータと従来コンピュータでそれぞれ得手の部分を担当して反復計算する変分量子固有値推定アルゴリズムがある。ここでは、文中で述べた n 量子ビットで 2^n 次元の行列を扱える点を活用して、量子コンピュータでそのような行列 (Hamiltonian) の 2 次形式計算が n の低次のオーダの時間で計算できることを活用する。

特集 Special Feature

では現在 15 量子ビットまでの種々の特徴を持ったマシンをフリーに使うことができる。その際には、5 量子ビットの場合なら、5 線譜に音符を書くようにゲートを配置して実行できる。そこで構成した量子回路を通して、ユニタリ行列を軸にした線形代数をある面学ぶこともできる。現在では、多くの IT ベンダがクラウドサービスの提供を開始しているところでもあり、習うより慣れろというだけではないが、今そこにある量子コンピュータシステムのサービスを使ってみない手はない。特に若手の方々は、現在のコンピュータが確立されて以来結構な年数を経ているところで、次世代の新奇のコンピュータの黎明期を楽しまない手はないのでは。ぜひ体験して未来を感じ、そして作っていただきたい。

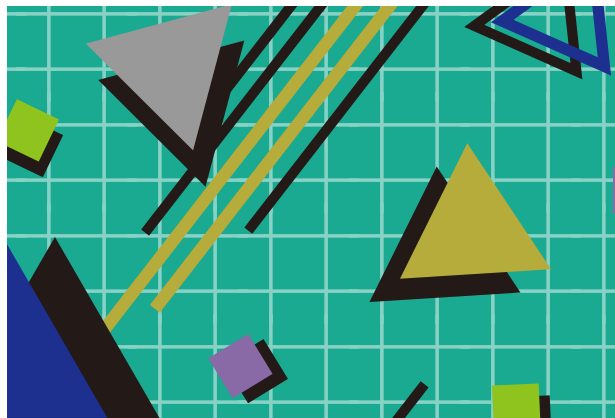
参考文献

- 1) Manin, Y. I : Classical Computing, Quantum Computing, and Shor's Factoring Algorithm. Ast'erisque, 266, S'eminaires Bourbaki, exp. No.862, pp.375-404 (2000).
- 2) Feynman, R. P. : Simulating Physics with Computers. Int. J. of Theore. Phys., 21, 6/7, 6, pp.467-488 (1982).
- 3) Shor, P. : Algorithms for Quantum Computation : Discrete Logarithms and Factoring. Proc. 35th Annual Symp. on Found. of Comp. Sci. (FOCS), pp.124-134 (1984).
- 4) Ito, T. and Vidick, T. : A Multi-prover Interactive Proof for NEXP Sound against Entangled Provers. Proc. 53rd Annual Symp. on Found. of Comp., pp.243-252 (2012).
- 5) Ji, Z., Natarajan, A., Vidick, T., Wright, J. and Yuen, H. : MIP*=RE. arXiv:2001.04383 (2020).

(2021 年 1 月 23 日受付)

■今井 浩 (正会員) imai@is.s.u-tokyo.ac.jp

東大計数工学科 1981 年卒業, 同情報工学専門課程 1986 年修了, 工学博士. 1986 年九大情報工学科助教授を経て, 1990 年より東大情報科学科, 現在東大情報理工学・コンピュータ科学専攻教授. JST ERATO 今井量子計算機構研究総括・同 ERATO-SORST (2000 ~ 2011 年). 本会量子ソフトウェア研究会主査.



[面白い量子技術]

② 量子アニーリングは死んだのか —研究の現状から思うこと—

基
般

大関真之 | 東北大学／東京工業大学／(株)シグマアイ

量子アニーリングとは何か

タイトルが衝撃的だったかもしれない。量子アニーリングを知っている読者からすれば、何が書いてあるのだろうという気になるだろう。しかし量子アニーリングを知らない読者も当然いらっしやるのだから、知らない読者のためにまずは量子アニーリングについて簡単に紹介しよう。量子アニーリングは組合せ最適化問題を解く手法として門脇正史氏、西森秀稔氏によって提案された。アニーリングという名前から想像されるようにシミュレーテッドアニーリングという方法と類似点が多い方法である。

組合せ最適化問題は、問題設定や条件に応じてコスト関数を定義し、そのコスト関数の最大化または最小化を目的とする。本稿では最小化を基本として紹介する。特に離散的な変数を持つ場合には、最小解を求める決定的な方法が乏しいため、さまざまなヒューリスティックが存在する。シミュレーテッドアニーリングは、その1つである。変数を動かしながら、コスト関数を下げる場合にはその変更を採択して、コスト関数が増える場合にはその変更を確率的に許容する。その確率については、コスト関数をエネルギーとして見立て、パラメータとして温度を導入して制御をする。非常にゆっくりとその温度パラメータを操作すると、各時刻では熱平衡状態に相当する確率分布を達成し、その確率分布は低温では低エネルギー状態が頻出するギブス・ボ

ルツマン分布となる。シミュレーテッドアニーリングは、こうした物理学で利用される特徴的な確率分布を利用した統計力学をその背景に持つ。

量子アニーリングは、同じように統計力学および量子力学を背景に持つ。量子力学を背景に持つというと、途端に読者は想像が追いつかないために、そつとページを閉じたくなるだろう。ただ量子アニーリングは、真に量子力学を使った手法とはいえない。そのため、想像が難しいことはない。

量子アニーリングの直感的理解

量子力学は恐るるに足らず

量子力学の教科書を読むと、その説明に「観測」という言葉があり、そしてその結果は「確率的」であるとする記述がある。つまり量子力学が述べる事実は、原子や分子など量子力学の適用範囲にあるものは、「観測」をしなければ、その結果を得ることができず、その結果が残念ながら決定的ではなく「確率的」であるという2つの観点で、我々の常識とはかけ離れているのである。我々には、世の中は観測するまでもなく、決定的に決まっているのが世の常だという思い込みがある。

実際には、目に飛び込むのは反射や散乱を繰り返してきた光子であり、その光子の情報から我々は色や強度を認識して脳内で画像化して認識している通り、観測行為をさりげなく行っているのだ。実験装置を仰々

しく用意するまでもなく、自然はそうした過程を通して私たちにその姿を初めて映し出す。その反射や散乱過程が量子力学により記述されるダイナミクスを伴い、観測されるまでに隠れてこっそり原子や分子を含めミクロな対象は、その状態をさまざまに変えているというわけだ。そのダイナミクスは自然のルールだから、実験結果を正確に再現するのであれば納得せざるを得ないことである。確率的であるということは、そこまで抵抗することではないはずだ。ノイズにより結果が乱雑に変化することを我々は往々にして確率的なモデル化を通して利用する。量子力学では、観測されるまでに裏で行われている自然のダイナミクスを記述するものが波動関数と呼ばれるもので、これは原子や分子のミクロな対象がどこに存在するのか、ではなく、さまざまな場所でどれほどの確率で存在するのかを計算する量である。確率振幅とも呼ばれる。

並行世界でのシミュレーテッドアニーリング

それでは量子アニーリングはどのように理解したらよいか。量子力学の確率的な要素を見やすくするための処方箋はいくつか存在する。実際に量子アニーリングをデジタルコンピュータ上で実装するために利用される量子モンテカルロ法を考えよう。量子モンテカルロ法では、仮想的な並行世界を鈴木・トロッター分解という方法の帰結として用意する。元々の対象とするコスト関数に付随する変数からなるシステムを、いくつか同じように用意する。この並行的に存在するシステムは、観測をした際に、どれか1つが選ばれた実現値を示している。理想的な量子力学では、この並行世界が無限個存在する。デジタルコンピュータ上では、そのような実現は不可能であるから、有限の並行世界をメモリの許す限り用意するのだ。このように説明すると、量子力学を利用したコンピュータに関する研究やデバイスが盛んに行われている理由が、次第に理解できよう。素朴に言えば無限のメモリが潜在的に存在するのが量子力学なのだ。さて量子アニーリングの話を進めよう。量子アニーリングでは、この

並行世界において初期条件として変数をすべてランダムに決めておく。この時点で観測する、すなわち並行世界のうち1つを選択すると、変数がバラバラの適当な値をとる。量子アニーリングでは初期条件として、さまざまな結果を重ね合わせた状態を用意する。この時点ではコスト関数の最小化はまったく意識されていない無作為な選択が行われる。ここから出発して、シミュレーテッドアニーリングのように、変数を変化させてコスト関数が下がれば採択、そして上昇した場合には確率的に許容する。その際に、隣接する並行世界との相互作用を与える。この相互作用の強さを次第に強くすることで、だんだんと並行世界の間で同じような実現値を取るようになる。最終的には、どの並行世界でも同じ状態となり、同じ答えを持つようになる。その結果を量子アニーリングの結果とする。これを量子アニーリングの解説では、量子揺らぎを強い状態から次第に弱めていくと表現している。量子揺らぎが強い状態では、さまざまな状態が結果として得られ、量子揺らぎが弱い状態では、我々の常識的な世界である、結果はいつも変わらない確定的なものとなる。

つまり量子アニーリングは、並行世界でのシミュレーテッドアニーリングと言って、差し支えがない。SF的な表現の好き嫌いはあるかもしれないが、実際に量子モンテカルロ法、またはデジタルコンピュータ上で量子アニーリングを実行する際には、並行世界を仮想的に用意していることは事実だ。

量子アニーリングの実現

D-Wave Systems 社の登場

そうしたデジタルコンピュータ上での仮想的な実装が量子アニーリングの提案時の様相であった。実際に門脇・西森の提案以降、量子アニーリングの研究では、シュレーディンガー方程式に基づく直球の数値的実験か、上記の量子モンテカルロ法によるシミュレーションによるものであった。本来であれば量子力学では、無限の並行世界を持つようなものであるが、

有限のリソースしか持たないデジタルコンピュータでは、そのシミュレーションは近似的であり、限界があったのだ。

しかしながら 2011 年、D-Wave Systems 社は量子アニーリングの実装を、量子力学の動作原理に基づく実機で果たした。つまり仮想的ではなく現実に無限の並行世界が存在するデバイスを用意したのだ。しかも商用販売を開始。世界で初めての「商用量子コンピュータ」として販売したのだ。歴史的には、量子アニーリングはシミュレーテッドアニーリングの改良版として提案されたものであり、量子コンピュータの文脈で提案されたわけでも、開発されたわけでもない。しかしこの D-Wave Systems 社の発表から世間的には、量子アニーリングの実装により、量子コンピュータが実現した、という見方が横行した。発表当初は懐疑的な見方が強かった。量子力学の原理に従い動作するデバイスで、量子アニーリングのように、量子揺らぎの強弱を変化させるだけの簡単な操作であっても実現することが信じられなかったのだ。D-Wave Systems 社からは次々と改良されたマシンが登場し、次第に学術論文という形で、量子アニーリングマシンで行われた実験結果を発表していった。懐疑的な見方は和らぎ、現在では量子力学の原理に従い動作することは間違いないだろうと落ち着いている。商用販売をしているというからには、顧客がいる。有名どころでは Lockheed Martin 社、NASA と Google 社の共同購入、Los Alamos 国立研究所や Oak Ridge 国立研究所などが大型クラウド契約を果たしている。大なり小なり、量子アニーリングを実行するマシンタイムを購入した企業や研究機関も存在し、日本からのユーザも非常に多い。

NASA と Google の記者会見

2015 年の年末に NASA と Google は第 3 世代の量子アニーリングマシン D-Wave 2X に関するベンチマークテストの結果を発表した。とある組合せ最適化問題について、シミュレーテッドアニーリング、および量子モンテカルロ法、そして D-Wave 2X に

よるベンチマークテストの結果を披露したのだ。シミュレーテッドアニーリングや量子モンテカルロ法に比べて、D-Wave 2X の方が最適解に到達するまでに必要とされる時間が 1 億倍ほど早いという内容であった。それを機に日本でも大々的に報道されるようになった。新聞のみならず Web メディアでも報じられ、テレビでもいくつか散見されるようになったのはこのころからである。

このベンチマークテストは、どのような問題であったのかというと、量子アニーリングは、シミュレーテッドアニーリングの改良として提案されたように、その出自は物理学からである。特にシミュレーテッドアニーリングも同様で、スピングラスと呼ばれる磁性体のシミュレーション技術の 1 つである。コスト関数はエネルギーに相当し、変数は、スピンと呼ばれる微小な磁石のようなものの向きを示す。上と下のみ、つまり 2 値のみを取る離散変数を持つ。ベンチマークテストでは、2 値の離散変数を持つ組合せ最適化問題を解いたというわけだ。確かに 2 値と言えど、連続値とは違い手がかりとなる微分がないため、基本的には手探りでありとあらゆる組合せを考慮する必要がある。計算量困難をはらむことは容易に想像がつかろう。それを 1 億倍早く解くと言われると確かに驚異である。実際に解いた問題は、ベンチマーク用に用意された特殊な組合せ最適化問題であった。シミュレーテッドアニーリングや量子モンテカルロ法では容易に解けないような問題を用意したのだ。具体的には 1 つの変数を変化させていく場合には、コスト関数が上昇してしまうことが多く、代わりに複数の変数を一気に変更するとコスト関数がようやく減少するような問題であったのだ。シミュレーテッドアニーリングや量子モンテカルロ法が極小の谷に喘いでいる中、量子アニーリングマシンは、容易に問題を解いてみせたという格好だ。ここで分かることは、量子アニーリングマシンは、極小の谷を抜け出しやすい性質があり、組合せ最適化問題を解くのに有利な影響を持つということである。ただしそうした有利な影響を持ち、シミュ

レーテッドアニーリングや量子モンテカルロ法に比べて有効であるということを示すためには、ある意味やらせの問題を用意する必要があったとも言える。

実際に後に人々の興味は、実際の応用上に必要な組合せ最適化問題での量子アニーリングマシンが示す性能に移った。興味が急激に高まり、量子アニーリングマシンが利用され、種々の組合せ最適化問題に適用されるようになった。しかしそれから次第に量子アニーリングマシンに関するネガティブな意見が散聞されるようになった。

量子アニーリングマシンの実際

ここで量子アニーリングマシンを触ったことのない人に向けて、どのような操作感で利用できるのかをお伝えしておく。量子アニーリングマシンは、その実機は基本的にはカナダの D-Wave Systems 社に置いている。初期には実機を導入した顧客も存在したが、現在ではメンテナンスの都合などから原則外には出さないポリシーとなっているようだ。大型クラウド契約や、時間貸しなどで多くのユーザがアクセスするサービスを展開している。そのため Web ブラウザ経由でアクセスしてログインやアカウント設定など、無償で公開されている Python 等の高水準言語で利用可能な D-Wave Ocean SDK (Software Development Kit) をインストールして、これに含まれる API (Application Programming Interface) にアクセスするトークンを発行すれば利用の準備が完了する。有料サービス以外にも、無料で 1 分間だけ量子アニーリングマシンを利用できるサービスがある。1 分だけと聞くと少ないと思うかもしれないが、量子アニーリングマシンは一度の計算は 20 マイクロ秒ほどである。その前後の前処理や後処理時間を含めると 100 ミリ秒ほどである。そのため 1 分と言えど使い切るには、何度も組合せ最適化問題を解く必要がある。

ライブラリには、量子アニーリングマシンに解きたい組合せ最適化問題のコスト関数を送付する関数などがある。コスト関数は制約なしの 2 次形式で書

かれる必要がある。その際に 2 次形式に伴う行列が得られ、その行列の数値データを基本的には送付することになる。その送信ののち、結果として 2 値のベクトルデータが得られて、手応えがあるやらないやら、とにかく答えが返ってくる。この時間は通信による遅延などもあるが大体 200 ミリ秒ほどである。現行の量子アニーリングマシンは D-Wave Advantage と呼ばれ、5,000 を超える量子ビットを持つ。この量子ビットは、並行世界で量子アニーリングを実際に実行する要素であり、1 つの量子ビットが 2 値の 1 つを表現し、どちらの値を取るのか、重ね合わせの状態をとった後に最終結果を返すのだ。

制約なしの 2 次関数のみを受け付けるので、制約ありの組合せ最適化問題は、少々書き換えを必要とする。等式制約であれば、等式を破るとコスト関数が上昇するように罰金法を導入すればよい。不等式制約についても、やや複雑ではあるが実装可能である。人々はありとあらゆる組合せ最適化問題を実装していった。5,000 を超える量子ビットを有するという事は、素直に受け取れば 5,000 変数の組合せ最適化問題が解けそうなものである。しかし実際には、これらのすべての変数の間に行列要素を直接埋めることができないのだ。量子アニーリングマシンの内部では、変数間の結合が限定的であり、現在では 15 個ほどの変数が 1 つの変数に関係づけられる。すべての変数間に係数を持つような行列が密な構造を持つ場合には、その実現は直接的にはできない。代わりにいくつかの変数をまとめて 1 つの変数を表すために無駄に量子ビットを利用することになる。

こうした事情のため、量子アニーリングマシンで一度に直接 5,000 変数の組合せ最適化問題を解かせるということとはできない。何度か分割して問題を解き、実効的に少ない変数の組合せ最適化問題を解いてもらうことになる。

これは決定的な弱点であり、そうした犠牲により、性能も悪化する。こうした背景もあり、よく分からないけれども「量子」なんとかというからにはすご

いのだろう、と浅はかな気持ちで参入した企業や研究機関は急速にガッカリモードに陥り、悪口を言うようになる。

D-Wave hybrid の登場

ユーザからはそうした諸問題を回避しながら、量子アニーリングマシンで実際に応用しようとする事例がいくつか提案されてきた。しかしその性能は果たして既存の数理最適化のアルゴリズムを大幅に超えるものであるのかどうか、そこに興味が注がれていった。2020年の2月末より D-Wave Systems 社からは D-Wave hybrid という量子アニーリングマシンとデジタルコンピュータが連動して大規模な組合せ最適化問題を解くサービスが登場した。当初1万変数の組合せ最適化問題を解くものであったが、現在では最大100万変数の組合せ最適化問題を解くことができる。それなりに大規模な問題を扱うので、計算時間も瞬時にというわけにはいかない。また問題の送信にも大きな行列の送信を伴うので、やや生成と時間がかかるようになる。先述の分割や実装上の工夫などを一切ユーザは気にせず、組合せ最適化問題を解くことができるので非常に有効なサービスではある。しかしいくつかのベンチマークテストを通して知ったことであるが、この D-Wave hybrid は、D-Wave Systems 社が用意したライブラリの中にある `neal.sampler`、無料で利用できるシミュレーテッドアニーリングを実装したものがあるのだが、それと大差のない性能を示す。有料と無料であれば、無料のものを利用する。しかも量子アニーリングとデジタルコンピュータによるハイブリッド計算システムであるとする、量子力学が純粋に効いたものであるというわけではないとすると、性能もさることながら、ブラックボックス的な様相をいよいよ持って感じるため、扱いづらいという側面もある。多少弁護すると、ここで実装されているシミュレーテッドアニーリングは非常に参考になる手法を採用している非常に優秀なものである。皮肉なことに非常に良い実装をしてしまったがために、基本的にはシミュレ-

テッドアニーリングで多くの組合せ最適化問題を、量子アニーリングを利用するまでもなく、解くことができるようになってきているのだ。

量子アニーリングのこれから

数理最適化ソルバとの比較

それでは量子アニーリングマシンの利用するメリットはあるのだろうか。現状ではないだろう。それは素朴な使い方をする限りでは現状存在しない。実際に既存の数理最適化ソルバとの比較を行ってみると、それはいよいよもって実感することである。たとえば Gurobi など有名な数理最適化ソルバと D-Wave hybrid を比較する。やってみればすぐに分かることだが、数理最適化ソルバの圧勝である。ただそれは当たり前のことである。数理最適化ソルバは離散変数の組合せ最適化問題を解く際に行っていることは、連続緩和して解き、離散変数を仮決めして、これまでに得られた解よりも悪化するなら、その可能性を切り捨てるといったことを繰り返して最適解を求めようとする。基本的には可能性を絞るという操作を途中で何度も行っている。また実行可能解の中で探索を行うことも可能である。しかし量子アニーリングでは、コスト関数には制約条件を満たすように罰金法を導入するのみで、探索するのは広大な全変数空間であることは変わらないので、量子アニーリングの探索能力がいかに優れようと、探索範囲が広すぎて無駄が多いのだ。実効的にハンデが大きすぎるのだ。そのため制約条件が多い問題では量子アニーリングマシンは圧倒的に不利となる。

さらに往々にして利用されがちであるが、線形計画問題を解くために量子アニーリングマシンを利用する例を多く聞くし、論文等公開されたもの以外でも、議論や研究発表等でも散見するが、これもやってはいけないことの1つである。量子アニーリングマシンは制約なしの2次形式の問題を直接解くことから、2次形式の問題を得意とする。わざわざ1次関数のみのコスト関数で、制約のある問題を解かせ

特集

Special Feature

るのは悪手である。実際数理最適化ソルバの前に屈服するのみである。逆に二次計画問題を解かせてみると、なるほど確かに素早くそれなりの答えを出してくる。ただ制約が多くなると次第に数理最適化ソルバに軍配が上がる。

そうした問題が量子アニーリングマシンは得意だとするとしても、前述の通り、今度はたちはだかる敵はシミュレーテッドアニーリングである。しかも D-Wave Systems 社の実装による、自前の実装によるものが立ちはだかるのだ。なんとも皮肉としか言いようがない。

そうやってできる問題とできない問題、得意な問題、不得意な問題を分類していくと限りなく量子アニーリングマシンならでは、という問題設定が少ないこと、皆無に近いことが見えてくるだろう。

種々のハイブリッドアルゴリズムの登場

量子アニーリングマシンとデジタルコンピュータの併用という方向性は、D-Wave Systems 社のみならず、ほかのユーザ企業や研究機関からも提案されている。数理最適化の手法として古くから知られる Benders 分解を利用したジョブショップスケジューリング問題を効率的に解く手法がコーネル大学や複数の研究機関からなるグループから提案された。ただこの方法は冷静に分析すると量子アニーリングマシンは不要であることには注意したい。この営み自体は、既存の数理最適化手法と量子アニーリングを組み合わせようとする態度について感心する。また連続緩和して大体の答えを掴み、0か1のどちらにするのが最終的に良いのかを判定するために量子アニーリングマシンを活用するというアルゴリズムが理化学研究所やデンソーから提案された。同種の発想は東芝から登場したシミュレーテッド分岐アルゴリズムにも見られる。連続緩和したシステムを考えて、自然のダイナミクスを量子アニーリングやシミュレーテッドアニーリング同様に導入して、最後の0か1のどちらにするのかというそのダイナミクス特有の分岐現

象を利用して決定する。実際に東芝のこのアルゴリズムを利用してデジタルコンピュータ上で実行すると非常に高速に効率的に最適解を得ることができる。また数理最適化の伝統的手法であるラグランジュ緩和と統計力学の計算手法であるハバード・ストラトノビッチ変換との関係を利用して、量子アニーリングマシンで罰金法による項を消去する方法が提案された。NTT データの研究者らはその改良により、組合せ最適化問題を実際に解ける水準にまで性能を向上させた。どれも数理最適化手法を、巧みに物理学を出自に持つシミュレーテッドアニーリングや量子アニーリングに組み込もうとする営みである。量子アニーリングは、これまでの研究に支えられて新展開を迎えようとしていることがうかがえる。

量子アニーリングマシンのあるべき姿

こうした取り組み以外にも、量子アニーリング、とりわけマシンの持つ意義をもう一度問いかけたい。組合せ最適化問題を解くために提案された手法であるから、その性能に興味が行くのは自然である。D-Wave Systems 社が量子アニーリングマシンを実装する前までは、純粋にシミュレーテッドアニーリングと比較した研究が多く見られた。ほとんどの例では量子アニーリングが優勢であるという結果が得られたのだ。その割には散々な結果であるとは言いようがない。それは量子アニーリングマシンに足枷がないような状況で、その性能を発揮させた研究がないことを意味する。前述したように解きたい組合せ最適化問題を載せるためにはさまざまな工夫を凝らして、実効的に扱える変数が少なくなってしまうこと、制約条件などは罰金法で実装するのだから、広大な探索範囲を持つとしても無駄に終わるといった弱点があるのだ。まずはこうした状況を理解して、やらせでなくてもよいから、量子アニーリングマシンの性能をつぶさに評価することが必要であろう。商用販売がなされ、産業応用に目を向けたために、そもそも量子アニーリングマシンとはなんだったのか？ ということを忘れていることが気にかかる。

特集 Special Feature

まずは制約なしの2次形式のコスト関数、またはそれに近い問題での利用をお勧めしたい。

さらに量子アニーリングそのものの有利な点を思い起こすと、やはりNASAとGoogleが示したことは重要である。たとえやらせの問題だとしても、多くの変数を同時に動かすような操作をしないと効率的に探索が行えないような問題で、量子アニーリングマシンは曲がりなりともその潜在能力を示すのだ。数理最適化ソルバが苦手とする問題は、シミュレーテッドアニーリングで、そして上記のような特筆すべき問題では、量子アニーリングを利用するという棲み分けがなされるのだろう。すべての問題を量子アニーリングマシンで解かなければならないわけではない。

さらに量子アニーリングマシンは、実際には理想的な量子アニーリングを実行できてはいない。多くの研究で指摘、確認されてきたことであるが、量子揺らぎの効果だけでなく、シミュレーテッドアニーリングで導入された温度の効果を無視することができない。これは完全に理想的な量子デバイスが実現しているわけではないことに由来する。そのためギブスボルツマン分布に従った結果を出力することが報告されている。機械学習で用意された学習データと同様なものを出力する生成モデルを学習する方法としてボルツマン機械学習がある。そこではギブスボルツマン分布に従ったサンプリングを必要とする。量子アニーリングマシンでは20マイクロ秒で1つの結果を出力する性質を駆使して、数百ミリ秒内に5,000量子ビットから数千のサンプルを作り出すことができる。しかもサンプル間の相関は非常に小さい。それはギブスボルツマン分布を生成させるために通常用いられるマルコフ連鎖モンテカルロ法のように、ある程度長い時間間隔を開けてサンプリングを行う方法とは違い、毎回毎回計算をやり直しサンプリングすることができるためである。毎回計算をやり直すとしても数百ミリ秒で終わるのであれば計算時間はさほど気にならない。

さらに量子アニーリングマシンでは量子揺らぎを強めてから弱めるという操作を行い、完全に量子揺らぎ

を切った場合の結果を得ることができない。これは理想的な量子アニーリングで期待される状況とは異なる。理想的な量子アニーリングでは完全に量子揺らぎを切ったものが期待される。これが原因で組合せ最適化問題の解法として利用した場合には、その精度を悪化させる要因ともなる。しかし量子力学に基づくデバイスとして考えると、その量子揺らぎの効果を検証する実験装置として活路が見出される。やや言い訳がましいものの、量子アニーリングは、マシンが登場して以降、組合せ最適化問題を解く以外にも、その利用方法が新しく見出され、想像の範囲を広げていったのだ。

量子超越性のニュースが2019年の秋頃に流れ、量子コンピュータの本道の研究がよいよ活況を迎えつつある。亜流として、はたまた邪道として見られてきた量子アニーリングに関するニュースはそうした意味で薄れていった。量子アニーリングは死んだかのようにすら感じるだろう。ある時期には量子アニーリングは紛い物扱いをするような言説が流れ、研究当事者として非常に辛い思いをしたことが懐かしい。ただ量子超越性の実験も、前述のNASAとGoogleなどの研究機関によって行われたものであり、そして再びある種の特別な設定で行われたものである。人々が興味を持って、多くの参入者を迎えたときに思わぬ使い道が導かれ、その方向性が伸びて、廃れてを繰り返す。その過程の真っ只中にいることを考えれば、死んだようにいて、実は死んだふりかもしれない。既存の手法と融合を重ね、量子アニーリングの本質的なことが多くの研究者によって発見されていくことで、復活してまた世間を賑わすことがあるかもしれない。もしくはそんなことはないかもしれない。それがどうした。研究をするというのは、そういうことだ。それでいいのだ。

(2021年1月23日受付)

■大関真之 mohzeki@tohoku.ac.jp

東北大学大学院情報科学研究科情報基礎科学専攻教授・東京工業大学科学技術創成研究院教授・(株)シグマイ代表取締役。東京工業大学大学院理工学研究科物性物理学専攻博士課程修了。京都大学大学院情報科学研究科助教。ローマ大学研究員。東北大学大学院情報科学研究科応用情報科学専攻准教授を経て現職。量子アニーリングと機械学習、スパースモデリング等のデータ駆動型科学の数理に関する研究に従事。

[面白い量子技術]

3 量子技術を利用した 次世代アクセラレータの活用

基
般

多和田雅師 | 早稲田大学

松田佳希 | (株) フィックスターズ

田中 宗 | 慶應義塾大学

楊 天任 | (株) QunaSys

量子技術を用いた 次世代アクセラレータの紹介

近年、量子技術を用いて計算を高速化する専用計算機の研究開発は大きな盛り上がりを見せている。専用計算機は次世代アクセラレータと呼ばれ、量子技術として量子アニーリング、Noisy Intermediate-Scale Quantum technology (NISQ)、誤り耐性量子計算 (Fault-Tolerant Quantum Computation, FTQC) の適用が期待されている。量子技術を用いた次世代アクセラレータの研究開発の盛り上がりの理由として大きく分けて社会ニーズと技術シーズの2つが挙げられる。第一に、社会ニーズ側の観点からの注目度の高まりである。Internet of Things (IoT) 技術をはじめとしたデータ収集の技術により、データの種類や量が膨大に増加している現在において、大規模データの高速高精度処理の実現が喫緊の課題である。その状況の中で、量子技術を用いた次世代アクセラレータが大規模データの高速高精度処理に資すると期待されているという側面がある。第二に、技術シーズ側の観点からの量子技術を用いた次世代アクセラレータ設計の現実感の高まりが挙げられる。量子技術を用いたアクセラレータ開発の基盤となる設計技術が着々と進化しており、実際に動作させることが可能な量子アニーリングマシンや NISQ デバイスが出て

きつつあるという側面がある。

量子技術を用いた代表的な次世代アクセラレータとして、量子アニーリングを用いるイジングマシン、NISQ デバイス、誤り耐性量子コンピュータについて、以下、簡単に概略を紹介する。

イジングマシンは、組合せ最適化問題の高効率解法が可能であると期待される次世代アクセラレータである。組合せ最適化問題とは、膨大な選択肢の中から、与えられた制約条件を満足し、かつ、目的関数を最大化（あるいは最小化）する選択肢を探索することを目的とした問題である。

NISQ デバイスは、誤り訂正がないアナログな量子コンピュータである。誤り訂正がないため、後に述べる誤り耐性量子コンピュータに比べれば性能が限定的になってしまうものの、NISQ デバイスを積極的に用いた産業・社会応用を可能にする理論枠組みの提案や NISQ デバイス実機を用いた検討が活発に行われてきている。

誤り耐性量子コンピュータは、量子技術を用いた次世代アクセラレータのハードウェア開発が現実的になるという想定の前から、情報科学と量子力学の境界領域としての研究として理論的な研究やアルゴリズム提案の研究がなされてきた。誤り耐性量子コンピュータの実現には大きなハードルがあるが、誤り耐性量子コンピュータを用いることを前提とした

特集 Special Feature

量子アルゴリズムの理論は数学的に保証されたものであるため、誤り耐性量子コンピュータが実現されたときのインパクトは計り知れない。

量子アニーリングやNISQについて、最近では量子コンピュータと古典コンピュータ（量子技術を用いない従来型コンピュータ）とのハイブリッド利用を念頭に置いたアルゴリズム提案や実機を用いた実験も進められている。これは、量子アニーリングやNISQが全体の情報処理の一部を高速化するアクセラレータとしての有用性を明確化するための重要な研究である。

以下、本稿の構成について述べる。まずイジングマシンの活用事例探索の研究開発について紹介し、次にNISQデバイスや誤り耐性量子コンピュータの活用事例探索の研究開発について紹介する。最後にこれらの量子技術を用いた次世代アクセラレータ基盤を構築する意義と最新の研究開発の現状について述べる。

イジングマシンの活用事例

量子アニーリング等のイジングマシンは統計物理学におけるイジング模型に代表される0-1整数二次計画問題の求解に特化したハードウェアである。すなわち、イジングマシンは、二値の決定変数に対する二次形式の目的関数を入力とし、目的関数が最小となる決定変数の近似解を出力する。高い汎用性を備えている一方で、任意の組合せ最適化問題に対してイジングマシンを適用するためには、与えられた問題を「二値変数」、「二次形式」の目的関数で表す必要がある。種々の組合せ最適化問題、とりわけNP完全・NP困難問題に対するこの「イジング定式化」の方法

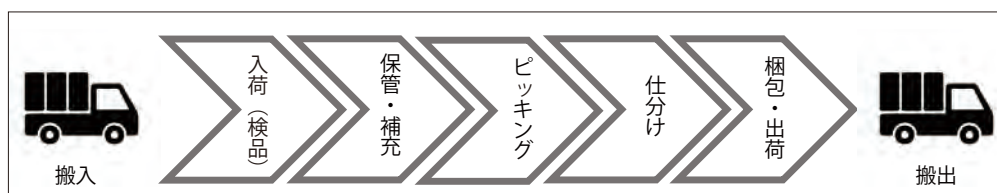
についての議論が活発に進められてきている。それらを基礎とした実問題における応用の例として、渋滞回避を目指した経路選択問題、工場内の無人搬送車の経路最適化、金融商品のポートフォリオ最適化、広告配信最適化、矩形パッキング問題、スロット配置問題、誘導部分グラフ同型問題など、多様な領域における組合せ最適化問題への取り組みがあり、イジングマシンによる処理が試みられている。本章では、そのような活用事例の1つとして、物流センターにおける人員配置最適化の取り組みとその実証実験の成果について紹介する。

物流センターの概要

本実証実験の対象とする物流センターは通信販売事業者専用の出荷センターである。約1,000人の従業員を擁し、1日あたり約30,000件の商品を出荷している。本物流センターにおける作業のプロセス（[図-1](#)参照）は次の通りである。通信販売業者から搬入された商品は、倉庫エリアに入庫され、検品が行われた後、保管エリアに移動される。商品は、消費者の注文に基づき、ある一定の単位の注文数ごとに保管エリアからのピッキング作業によりまとめられる。その後、最終工程である梱包エリアにて消費者ごとに商品が梱包され出荷される。作業者は各エリアに独立して作業しており、作業場所あるいは作業分類に基づき担当作業が割り当てられる。この割り当てが、物流センターにおける作業者の人員配置計画である。

人員配置の最適化

本物流センターにおける人員配置計画は日々の重要な業務の1つである。なぜなら各作業に対する適切な担当者の決定が、物流センターにおける全体の



■図-1 本物流センターにおける主要業務プロセス

特集 Special Feature

効率性に影響を及ぼすためである。日々の注文によって計算される各業務の目標量を達成するために、当日の出勤者名簿、そしてその名簿に基づく作業者の作業可能量を考慮した人員配置計画が行われる。

実証実験では、イジングマシンを用いた人員配置計画の最適化を目的とする。そのためには、何を最適化するのかについて現実に即した妥当な定義を行い、それを定量的に数式で表現する必要がある。業務における目標量を達成するという指標においては、達成度合いの充足率を最大化することで定義されるのが自然である。本実証実験では図-2のようにコスト削減に直結する作業数数の最小化というよりは、与えられた目標量を満たしつつ、従業員全体での負担軽減・負荷の均等化に資する「効率の良い配置と作業工数の平等化」に着目した人員配置計画を提示するものである。

一方で高い精度で充足率を推定するには、各作業者の作業可能量（スキル）の見積もりが重要になる。本物流センターでは、作業者はハンディターミナルを用いて作業管理を行っており、そのデータは倉庫管理システム（WMS）に蓄積される仕組みを持っている。このデータを用いると、各作業者の単位時間あたりの作業可能量の推定が可能となり、これをスキル値とする。すなわち、各作業における担当作業者のスキル値の合計に勤務時間を掛けた値は、ある

人員配置における1日あたりの作業可能量の見積もりとして有効である。

実証実験

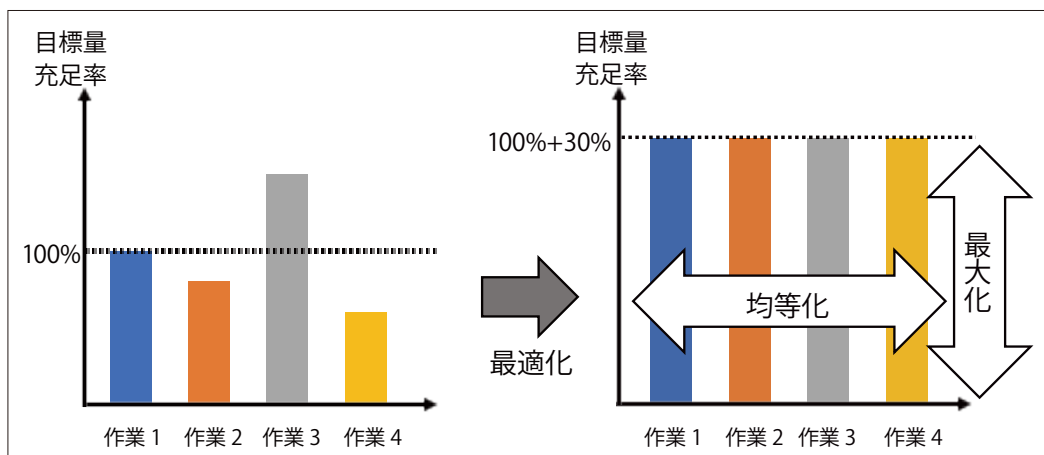
本実証実験では、物流センターの業務のうち梱包・出荷エリアの作業者約100人を対象として、作業種ごとに与えられる目標量に対し適切な人員配置表の作成を行った。

梱包・出荷エリアの作業は次の4種類に分類される。

- 単伝：1つの出荷先に1つの商品を梱包して出荷
- 復伝：1つの出荷先に複数の商品を梱包して出荷
- ギフト単伝：上記の単伝にギフトラッピングを施す
- ギフト復伝：上記の復伝にギフトラッピングを施す

このうちギフト梱包に関してはラッピングの技術が必要であり難易度が高い。つまりすべての作業員が担当可能ではない業務が存在する。それぞれの業務に対して目標量が設定され、与えられた作業者の名簿に基づき午前・午後それぞれのスロットに4種類どの作業を担当するのかを決定する。

イジングマシンの実行に必要な定数は次のようにして設定を行った。まず、作業者ごとにそれぞれの業務の作業可能量、すなわちスキル値の見積もりが必要である。今回の実証においては2019年7月1日



■図-2 作業の目標量の充足率最大化と作業間の充足率の分散の均等化について模式図。作業1～4は、本物流センターにおける単伝、復伝、ギフト単伝、ギフト復伝の4種類の作業に対応する。

～7月10日までの梱包実績データから、この作業に一度でも従事した238名の4種類の作業種別の実績数を30分ごとに集計し、その平均値を各個人のスキル値とした。前述のように、ギフト梱包が担当可能な作業員以外はギフト梱包のスキル値を0とする。最適化の効果を確認するために、2019年7月1日の作業実績データを比較対象とし、作業ごとの目標量の設定や作業員人数100名、その他の定式化に必要な定数についてもこの過去実績を参照した。

上記の問題設定を定式化すると決定変数が800変数(100人×4種類×午前午後2スロット)の二次式となる。今回はFixstars製イジングマシン「Optigan」を使用し実行タイムアウト時間100msで最適化を試みた。最適化結果の人員配置計画を用いた充足率は表-1の通りである。

過去の人員配置計画による実績では充足率がおおむね100%だったのに対し、上図の人員配置を用いることで、4種類の作業のどれもが30%弱の時間的猶予を持ち得るという推定結果を表している。また、業務間の充足率の均等化もほぼ認められるものであり、前述の定式化が機能していることを示唆する結果となっている。

本実証実験では、イジングマシンを用いて組合せ最適化問題を解くことにより、実問題を高速かつ高精度に処理することができる可能性について示した。イジングマシンは一般にヒューリスティクスであり、最適解ではなくとも実用性の高い解を迅速に見つけることによって新たなソリューションを提供できる可能性があると考えられる。計算技術や情報処理能力の発展と、業務プロセスにおけるDX推進などの取り組みと継続的に連携していくことが、今後新たな価値を創出するために重要であると考えられる。

■表-1 イジングマシンを用いた各作業に対する人員配置の充足率

	単伝	復伝	ギフト単伝	ギフト復伝
充足率	127.5%	127.5%	128.1%	129.4%

NISQ デバイスと誤り耐性量子コンピュータの活用事例

本章では、NISQ技術を用いるNISQデバイスと誤り耐性量子計算(FTQC)技術を用いる誤り耐性量子コンピュータについて、最新の動向を紹介する。

NISQデバイスと誤り耐性量子コンピュータはともに「ゲート式量子コンピュータ」に対して使われる呼称であり、これはイジングマシンのような特定の問題に特化した計算機ではなく、汎用的に計算を行うことを目的とした計算機である。これは問題特化型のマシンと比較して実装の難易度が高いことを意味しており、イジングマシンとゲート式量子コンピュータは、活用フェーズが異なる。

NISQデバイスと誤り耐性量子コンピュータは、誤り訂正のあり・なしで区別される。量子コンピュータの応用先として話題にあがる、暗号解読や全探索、Full-CI計算などのパワフルなアルゴリズムを実行するためには、誤り訂正機構を持った大規模な量子コンピュータが必須である。

一方で、近年Googleが53qubitのデバイスを作って量子超越¹⁾を発表するなど、大規模な量子コンピュータの実現に向け、不完全なデバイスをうまく使いこなして必要なマイルストーンを達成しようという潮流がある。誤り訂正機能がないこのような量子コンピュータはNoisy Intermediate-Scale Quantum (NISQ) デバイス²⁾と呼ばれている。

NISQデバイスの特徴としては

1. エラー訂正がされてないため、計算を途中で間違えることがある (Noisy)
 2. 50～1,000qubit程度のデバイスである (Intermediate-Scale)
- という点が挙げられる。

ここで重要なのは、FTQCの古典コンピュータに対する優位性は理論的に証明されているが、NISQの優位性は理論的には証明されていないということである。ゲート式量子コンピュータにおいては、その事

特集 Special Feature

実は踏まえつつ、FTQC の到来を待たずに、NISQ をうまく使いこなす、より早い時期から量子のアドバンテージを享受しようという考えの下、マシンの開発やアプリケーションの検証が進められている。そのアドバンテージの達成が、「量子加速」と呼ばれるマイルストーンであり、これは2020年12月時点ではいまだ達成されていない。現在活用が期待されている領域を図-3に示す。ゲート式量子コンピュータの適用領域は、現時点では広くなく、対象となる計算を実行できる量子アルゴリズムが存在するかどうかで決まっている。FTQC で量子加速が約束されているのは量子化学、機械学習、最適化、暗号解読、微分方程式であり、その内 NISQ フェーズで量子加速が一定期待されているのは量子化学、機械学習、最適化の3つである。裏を返せば、アルゴリズム次第で適用領域は広げることができるということであり、ハードウェアの開発と同様、アルゴリズム開発も重要であるといえる。

現在提案されている応用先の中で、最も市場の立ち上がり（＝量子アドバンテージを享受できる時期）の到来が早く、さらにインパクトが見込めるのは、量子化学計算とされる。また長期的には、素因数分解を多項式時間で解くことによる「暗号解読」が一番のキラアプリケーションとなると考えられるものの、実現はかなり先になると予想される。一般的な公開鍵暗号である RSA2048 を破るのには、2,000 万

physical qubit³⁾ が必要である。このようなデバイスの実現には、どんなに楽観的に見積もっても、あと10年かかるであろうと考えられている。

いずれにせよ、現段階で実現しているハードウェアは50qubit程度であり、暗号解読はおろか、最も早い立ち上がりが見込まれるとされる量子化学計算ですら優位性は示されていない。現在は、量子コンピュータの振る舞いを古典コンピュータ上で再現したシミュレータを使ってアルゴリズムの開発や検証を行うとともに、実機上で簡単な系を動かすことにより、各種アルゴリズムの性能検証や実機制御ノウハウの蓄積などが進められている。

現在の取り組みプレイヤーの概観は、図-4のとおりとなる。量子コンピュータは分野として発展途上であり、古典コンピュータの世界ほど各レイヤの分業が進んでいない。将来的には、各レイヤがさらに細分化され、水平分業が進むことが想定される。

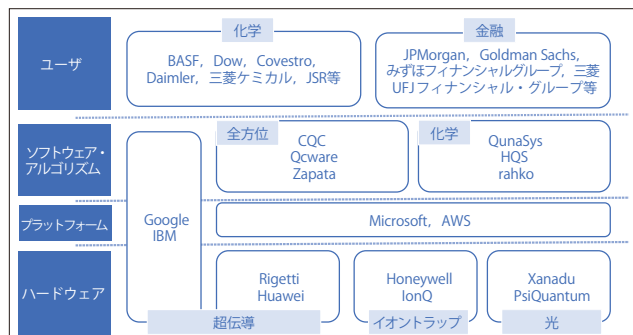
ユーザ企業はどのような分野での活用を見据えて、ユースケース探索を行っているのだろうか。代表的な取り組みを図-5に示す。

化学の分野においては独 Covestro が触媒材料への応用を見据えてアルゴリズム開発等を進めている。また、同じく EU においては、英 Johnson-Matthey が政府系プロジェクト通じて電池や触媒材料への応用を見据えて検証に取り組む。また、国内では三菱ケミカルが光化学反応解析への応用を見据えて取り組みを進めている。

QunaSys は化学計算で活用可能なアルゴリズムの



■図-3 NISQ と FTQC のアプリケーション



■図-4 取り組みプレイヤー概観

特集 Special Feature

開発に焦点をあてて活動を行っており、化学計算を行う上で重要な励起エネルギーやエネルギー微分等の物性値を求めるためのアルゴリズムを提案している。これらはまだ古典に対するアドバンテージを示すには至っていないが、今後はユーザ企業と協働してこれらアルゴリズムを適用し、最初の実用例を作っていく。

また、化学・材料分野だけでなく、製薬業界でも量子コンピュータ活用が期待されている。特に、北米においては QuPharm という製薬企業の協調領域のコンソーシアムが立ち上がっており（2020年12月時点）、ここで各社勉強・議論を進めながらユースケースの見極めを行っている。

また、それ以外の領域では、独 BMW やフォルクスワーゲンなどが交通最適化や電池材料への応用を期待して PoC (Proof of Concept) を進めているほか、金融業界の名だたるプレイヤーが、ポートフォリオ最適化やデリバティブの価格付け等への応用を見据えてアルゴリズム開発や PoC を進めている。いずれの領域でも、実際に事業で量子コンピュータを活用しているわけではなく、量子コンピュータ利用の検証が進められている段階となっている。このような取り組みの中から、2～3年後に最初の実用例が生まれ、そこから活用が進んでいくことが期待されている。

ゲート式量子コンピュータは、「活用」という観点では発展途上の技術である。NISQ フェーズでは、

小さくてよいので何か次に繋がる成果を示すことが重要となる。おそらく、NISQ フェーズである程度の有用性が示されなければ、それ以上は研究開発投資が続かず、人類は FTQC のもたらす大きなアドバンテージを享受することはできないだろう。NISQ を使いこなして何かしらの実用例を示し、産学のプレイヤーを呼び込み、数多くの活用事例を蓄積することが、量子コンピュータ技術の発展のためには必要不可欠だ。同じように考える熱心なプレイヤーが、最初の実用例の発掘を目指し、今日研究開発に取り組んでいる。非常にリスクが高く、チャレンジングな試みではあるが、その先には大きな可能性が広がっている。

次世代アクセラレータ基盤

協調設計の必要性

本章では量子技術を取り扱う次世代アクセラレータ基盤意義と最新の研究動向を説明する。次世代アクセラレータはあらゆる計算に万能に有効ではなくそれぞれ得意とするアプリケーションが異なると考えられるが、得意不得意の判定は専門的な知識を必要とし次世代アクセラレータを使用する上での障壁となっている。これまで述べたようにイジングマシン、NISQ デバイス、誤り耐性量子コンピュータを活用するためには高い専門性が求められる。次世代アクセラレータごとにソフトウェア開発は進められおり、専門的な知識を必要とせず特定の問題に対して特定の次世代アクセラレータを使用することは比較的容易になっている。しかしながら、大きなスケールのアプリケーションを実行できる実機が存在しないため、あらゆるアプリケーションに対してソフトウェア開発が十分進んでいるとは言えない。特に種別をまたいで実行する次世代アクセラレータを選択するソフトウェアフレームワークは研究されておらず、次世代アクセラレータの使いやすさを高めることが急務である。ユーザが専門知識を持たないまま、使用するアクセラレータの選択を気にすることなく

企業名とこれまでの取り組み概要

化学	Covestro	<ul style="list-style-type: none"> 2020年7月、Googleとの協業を発表 触媒材料等への活用を見据え、計算アルゴリズムの開発等に取り組む
	Johnson-Matthey	<ul style="list-style-type: none"> 2020年よりUKの国プロに参画 電池材料、および触媒材料を対象として、有効性を検証中
自動車	BMW	<ul style="list-style-type: none"> 2018年よりPoCを開始 配車マッチングや電池材料計算で、有効性を検証中
金融	JPMorgan	<ul style="list-style-type: none"> ポートフォリオ最適化、デリバティブの価格付け等への活用を見据え、各種検証やアルゴリズム開発を進める

■図-5 主要プレイヤーの取り組み

プログラムの実行が可能となるソフトウェアの開発が必要である。

最新の研究開発の現状

イジングマシン、NISQ デバイス、誤り耐性量子コンピュータは必ずしも古典コンピュータよりすべてにおいて勝っているわけではない。そのためハイブリッドな実行が必要不可欠となる。大きなプログラムを構成する小さなプログラム（部分プログラム）に対して次世代アクセラレータを割り当てる次世代アクセラレータ・コデザイン問題が研究されている。

次世代アクセラレータ・コデザイン問題は定式化が示されており、静的に割り当てが可能ならばこれはスケジューリング問題の一種と見なすことができるが実用上は部分プログラムに次世代アクセラレータを割り当てた場合の実行時間等変数を事前に得ることができないという課題が存在する。そのため次世代アクセラレータによる部分プログラムの実行時間や実行結果の品質を推定する研究開発が進められている。各次世代アクセラレータに対しプログラムの入力が与えられたときの推定方法は、いくつかはすでに発表されさらなる成果が期待できる。今後はプログラムの動的な実行を最適化するソフトウェアそのものの研究開発を進める方針である。

謝辞 本研究の一部は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム (SIP)「光・量子を活用した Society 5.0 実現化技術」(管理法人:量子科学技術研究開発機構)によって実施された。

参考文献

- 1) Arute, F., et al. : Quantum Supremacy Using A Programmable Superconducting Processor, Nature, Vol.574, pp.505-510(2019).
- 2) Preskill, J. : Quantum Computing in The NISQ Era and Beyond, Quantum, Vol.2 (2018).
- 3) Gidney, C. and Eker, M. : How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits, arXiv: 1905.09749 (2020).

(2020年12月28日受付)

■多和田雅師 (正会員) tawada@togawa.cs.waseda.ac.jp

2015年早稲田大学大学院基幹理工学研究科博士後期課程修了。博士(工学)。現在、早稲田大学グリーン・コンピューティング・システム研究機構次席研究員。専門は計算機システム設計。

■田中 宗 (正会員) shu.tanaka@appi.keio.ac.jp

2008年東京大学にて博士(理学)取得後、東京大学、近畿大学、京都大学、早稲田大学を経て、2020年より慶應義塾大学理工学部物理情報工学科准教授。専門は量子アニーリング等イジングマシン、統計力学。

■松田佳希 y_matsuda@fixstars.com

2011年東京工業大学大学院理工学研究科物性物理学専攻博士課程修了。2013年(株)フィックスターズ入社、現職。2020年早稲田大学グリーン・コンピューティング・システム研究機構 客員次席研究員(講師)。

■楊 天任 (正会員) yan@qunasy.com

2016年に東京大学工学部機械情報工学科を卒業し、同大学院の情報理工学系研究科知能機械情報学専攻に進学し、現在休学中。2018年に(株)QunaSysを設立し、量子コンピュータの用途を広げるアルゴリズム研究を行いながら、量子コンピュータを利用するためのソフトウェア開発に取り組んでいる。



[面白い量子技術]

4 量子コンピュータを用いた金融計算



宇野隼平 | みずほ情報総研 (株)

金融とコンピュータ

金融業務におけるコンピュータ利用の歴史は長く、1950年代から大型計算機を導入し、主に勘定系のシステムなどで膨大な情報処理を行ってきた。また、近年では、インターネットやスマートフォンの普及によるライフスタイルの変化、FinTechの流行、他業種による金融サービスへの参入の影響等もあり、コンピュータによる情報処理を活用して金融を便利にする革新的なサービスが次々と生み出されている¹⁾。具体的には、たとえば、AIを利用して投資や運用の支援をするロボアドバイザー、コンピュータを用いて自動的に取引を行うアルゴリズム取引、ブロックチェーン技術による仮想通貨等が挙げられる。こうしたサービスでは、顧客情報や取引データ等の大量の情報を高速に処理する必要があり、情報化社会の進展を考慮すると、今後さらに莫大な計算能力が必要になると予想される。

こうした金融サービス以外に、安定的な金融システムの確保や金融犯罪の防止等にも、今後多くの計算処理が必要になることが考えられる。たとえば、規制の強化の方向として、シミュレーションにより保有する資産のリスクを評価する、大量の取引の中から不正取引やマネーロンダリングを検出する、というような計算の必要性が議論されている。

金融業界では、こうした将来的な計算量の増大に備えて、近年、量子コンピュータの活用を検討し

ている。国内においては、2018年に慶應義塾大学にIBM Q Network Hubが設立され、筆者の所属するみずほが参画し、三菱UFJフィナンシャル・グループや三井住友信託銀行とともに量子コンピュータの活用の研究を行っているほか、海外においても、IBM Q Networkに参加しているJPMorgan ChaseやGoldman Sachs等をはじめ、さまざまな金融機関が将来的な活用に向けた研究を積極的に行っている。

本稿では、金融機関における量子コンピュータ活用に向けた取り組みのうち、特にデリバティブ（金融派生商品）の価格評価を中心に解説を行う。その他、金融計算への量子コンピュータの適用先として検討されている、最適化、機械学習等に関しては簡単に触れるにとどめる。最適化、機械学習等の詳細については最近のレビュー²⁾を参照のこと。

デリバティブ価格評価と量子計算

金融商品には、株価や為替レートなどの商品（原資産）から派生したデリバティブ（金融派生商品）と呼ばれる商品がある。デリバティブは、原資産の価格変動による損失のリスク回避、リスクを負った収益性の追求等、さまざまなリスク選好に対応するために考案された商品である。デリバティブの適正な価格を算出するためには、株価などの原資産の価格変動の履歴をサンプルするモンテカルロ・シミュレーションが用いられることが多い。モンテカルロ・

特集 Special Feature

シミュレーションでは、計算の誤差を十分小さくするためには大量のサンプルを発生させる必要があり、このため、デリバティブの価格評価は金融機関において最も時間を要する計算の1つとなっている。

量子コンピュータでは、デリバティブ価格評価の計算コストを大幅に削減することが可能なアルゴリズムが知られている。ここでは、デリバティブ価格評価と量子アルゴリズムの概要と、量子アルゴリズムを少しでも早く活用するために筆者らが行ってきた最近の研究について紹介する。

金融工学とデリバティブ

株価や為替レート等はあらかじめ決まった価格で売買されているのではなく、毎日のニュースなどで報じられるように時々刻々と価格が変化する。これらの金融商品（デリバティブと対比して原資産と呼ばれる）の価格は市場の参加者の需要（買手）と供給（売手）のバランスにより決まる。たとえば、企業の業績が好調だと判断した買手が売手に対して多

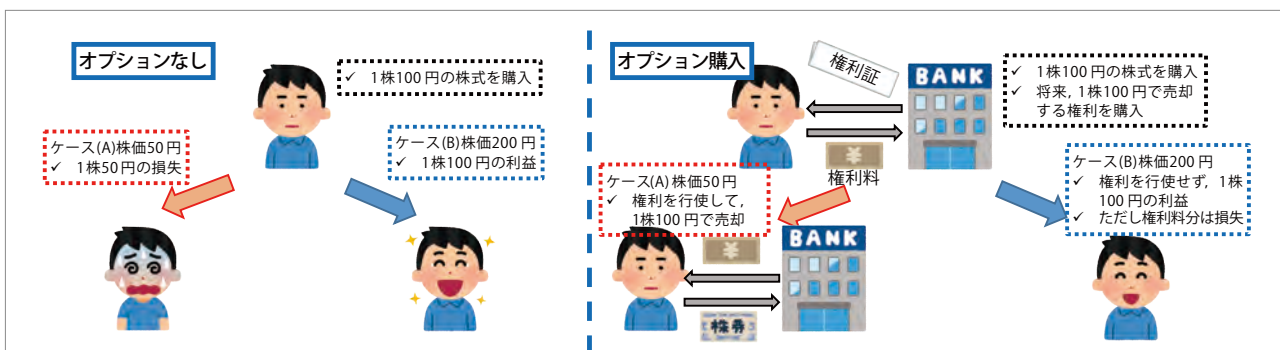
い場合には、株式の需要が高まり、一般には株価は上昇するといった具合である。

原資産価格の変動は、企業業績や社会情勢等により説明できることもあるが、ほとんどの場合には、多くの市場参加者のさまざまな思惑により、きわめて不規則に変動する。このため、価格の変化の動きを予測することはきわめて困難である。

株式などの原資産の所有者は価格の大幅な上昇により利益を得る可能性がある一方で、予測できない大暴落等により大きな損失を被るリスクがある。このようなリスク（不確実性）をコントロールして、さらに大きな利益を追求したり、リスクを回避したりするために、原資産の価格に依存して価値が決まる「デリバティブ」と呼ばれる金融商品が使われている（図-1）。たとえば、未来が予測できない中で、利益を得る可能性を残しつつ、損失を負うリスクを回避するのに使用されるデリバティブとして、オプションと呼ばれる金融商品がある。オプションは、将来のある時点（または期間）において、原資産を取引する権利のことである。定義だけだと分かりづらいので、具体例として、現在1株100円の株式を購入したときに、オプションとして「1年後にこの株式を1株100円で売る権利」を購入することを考える（このように特定の日に、特定の価格で売る権利をヨーロピアンputオプションという）。これは株価下落のリスクに備えていることになる（図-2）。このような権利により、たとえば株価が大幅に下落した（たとえば1株50円になった）



■図-1 デリバティブ（金融派生商品）の種類



■図-2 オプションによるリスク回避の例

としても、株式を100円で売ることができ、損失を負わない。一方で、株価が大幅に上昇した（たとえば1株200円になった）場合には、権利を放棄して株式を直接売却することで、大きな利益を得ることも可能となる。もちろん、ただでリスクを回避することが可能になるというわけではなく、「権利」の購入には一定の手数料、オプションとして適切な価格を支払う必要がある。この権利の価格はいくりにするのが適切であろうか？ この価格を決定する方法を与えるのが、金融工学（数理ファイナンス）である。

金融工学では、原資産価格の予測不可能な不規則な変動を確率的な変動、確率過程としてモデル化する。ちなみに、モデル化を行うことで、確率的に莫大な利益があげられるようになる、というわけではない。金融工学では、確率的な議論をうまく利用し、適切なデリバティブの価格付を行うことで、販売する金融機関が不利益を被らない（損をしない）ことが可能となる。

裁定機会とリスク中立確率

金融工学におけるデリバティブの価格付理論によれば、デリバティブ価格は、原資産価格がある擬似的な確率（「リスク中立確率」と呼ばれる）で変動した場合の将来的な価値の期待値を取ることで算出することが可能となる。この価格算出手法の導出には比較的複雑な手順が必要となるため、ここでは主な前提条件と結果のみを示す。興味のある読者は金融工学の教科書³⁾を参照のこと。

デリバティブ価格算出で重要な仮定は、市場に裁定機会がないということであるということである。「裁定機会」とは、リスクなしに、確実に収益を得ることができる機会である。たとえば、ある企業の株式が、市場Aより市場Bで高額で取引されているとすると、その株式を安価な市場Bで購入し、市場Aで売却をすれば、リスクなしで利益をあげる裁定が可能となる。もしも、このような裁定

機会があるとした場合、多くの市場利用者がこれを利用することとなるため、裁定がなくなる方向に価格が是正され、速やかに無裁定に近い状態になると考えられる。このため、ごく短期の裁定機会を除いて、ほとんどの場合において、市場は裁定機会がないことが仮定される。

ここでは詳細に踏み込まないが、「裁定機会がない」ことに加えていくつかの仮定を置くと、デリバティブの適切な価格がある種の確率の下での期待値として算出される。もし、このようにして決められる価格から大きく離れた価格をつけたとすると、裁定機会が発生してしまい、金融機関は大きな損害を被る可能性があり、このため、適切な価格を算出することは重要な課題である。以下では、従来型のコンピュータ、量子コンピュータのそれぞれにおける期待値の算出手法について概説する。

既存コンピュータでの期待値計算

前述のように、デリバティブの価格評価には、ある確率の下での期待値を計算する必要があるが、ごく一部の単純な場合を除き、多くの現実的なケースでは、解析解を得るのは困難である。このため、近年のコンピュータ能力の大幅な向上も相まって、数値的に期待値を近似的に評価する方法が発展してきた。

簡単に言ってしまうと、期待値計算は確率変数の次元を d とすると、 d 次元ベクトル $\mathbf{x}=(x_1, x_2, \dots, x_d)$ 上の関数 $f(\mathbf{x})$ の単位区間 $[0,1]^d$ 内での定積分

$$I(f) = \int_{[0,1]^d} f(\mathbf{x}) d\mathbf{x} \quad (1)$$

の近似値を求める問題である。（なお、以下では簡単のため、関数 $f(\mathbf{x})$ は、区間 $[0,1]^d$ において $0 \leq f(\mathbf{x}) \leq 1$ を満たし、かつ、滑らかな関数であることを仮定している）。近似値を求めるにあたっては、任意のサンプル点 \mathbf{x} に対して、関数値 $f(\mathbf{x})$ の値が算出可能だとする。一般に、関数 f は呼ばれるごとにコストがかかり、このため、アルゴリズムの

計算コストは、 f の呼び出し回数 (= サンプル点数) で評価できる (その他の計算コストは無視する)。ある一定のコストに対して、最も良い精度で積分の近似値を得ることが数値計算の目標である。

最も単純な方法としては、変数の各次元を区切って、関数の値を近似する方法が考えられる。たとえば、中点近似では、各 d 次元の $[0,1]$ の区間を m 等分にすることで、式 (1) の積分 $I(f)$ を以下のように近似する。

$$I(f) \sim S(f) = \frac{1}{m^d} \sum_{i \in J} g(i) \quad (2)$$

ここで $J = \{1, 2, \dots, m-1\}$, $g(i) = g(i_1, i_2, \dots, i_d) = f\left(\frac{i_1}{m} + \frac{1}{2}, \frac{i_2}{m} + \frac{1}{2}, \dots, \frac{i_d}{m} + \frac{1}{2}\right)$ とおいた。中点近似では、誤差 ϵ を達成するのに必要なサンプル点の個数は $O(\epsilon^{-d/2})$ と、次元 d に対して指数関数的に依存しており、いわゆる“次元の呪い”に陥っている。たとえば $d=100$ として、誤差 $\epsilon=10^{-3}$ を達成したいとすると、 $O(10^{150})$ 個程度と莫大なサンプル点 (関数 f の呼び出し) が必要となる。これは、 f の呼び出しに要する計算が 1flop (浮動小数点計算) であり、さらに、今後登場する Eflops 級 (1 秒間に 10^{18} 回浮動小数計算を行える) のスパコンを利用できるという楽天的な仮定をおいたとしても、実行に必要な時間は $O(10^{125})$ 年程度となり、現実的に実行するのは不可能な計算コストである。典型的な金融の問題では、確率変数の個数は数百次元に及ぶため、中点近似で期待値の計算を行うのは現実的ではない。

そこで、高次元の問題においては、モンテカルロ法が使われるのが一般的である。モンテカルロ法では、 N 個のランダムなサンプル $\{x_1, x_2, \dots, x_N\}$ を用いて、以下のように近似値の計算を行う。

$$I(f) \sim \frac{1}{N} \sum_{i=1}^N f(x_i) \quad (3)$$

この近似における誤差 ϵ とサンプル数 N の関係は、中心極限定理により、 $N=O(1/\epsilon^2)$ と次元に依らなくなり、次元の呪いを回避することができる。特に、モンテカルロ法は被積分変数の次元 d が大

きい場合のほぼ最適なアルゴリズムであることが知られている。なお、モンテカルロ法による計算 (式 (3)) が、中点近似 (式 (2)) に較べて大幅に改善した定性的な理由としては、中点近似では近似精度が最悪の場合に誤差がいくらになるかを示しているのに対して、モンテカルロ法では平均的な誤差 (最悪の場合にはこの誤差を遥かに超える) を議論しているためである。

量子コンピュータでの期待値計算

モンテカルロ法は、確率変数の次元に依らないため、高次元の積分計算をある程度短い時間で実行可能であるが、現実的には、必要な計算コスト (関数 f の呼び出し回数) $N=O(1/\epsilon^2)$ は非常に大きい。このため、モンテカルロ計算は、金融だけでなく、物理シミュレーションなどさまざまな分野で、最も多くの時間を要する計算の1つとなっている。一方で、量子コンピュータでは、必要なコストを $N=O(1/\epsilon)$ 程度まで減らせるような、アルゴリズムが知られている。このアルゴリズムは、非常に多くの複雑な演算が必要であるため、今後しばらくの間のノイズのある量子コンピュータで実行するのは困難である。このゲート演算を減らし、少しでも早く振幅推定アルゴリズムを活用するために、近年、筆者らはアルゴリズムの改良を行ってきた。ここでは、これらの量子アルゴリズムについて紹介を行う。

まず、既存の振幅推定を用いた量子アルゴリズムについて概説する。振幅推定を使った期待値推定の量子アルゴリズムでは、本来求めたい式 (1) の積分ではなく、式 (2) の中点近似値に対する推定を行う。中点近似として、 d 次元積分の各次元を $m=2^l$ 分割するとする。 $l \times d$ 次元のビット列 i で表すとすると、量子コンピュータ上ではこれらのビット列の重ね合わせ状態 $\frac{1}{m^{d/2}} \sum_{i \in J^d} |i\rangle$ を作成することが可能である。この重ね合わせ状態に 1 ビットの補助ビット $|0\rangle$ を加えた状態 $\frac{1}{m^{d/2}} \sum_{i \in J^d} |i\rangle |0\rangle$ に対して、以下のように $g(i)$ を並列的に作用するような演算を

仮定する.

$$\frac{1}{m^{d/2}} \sum_{i \in I} |i\rangle|0\rangle \rightarrow \frac{1}{m^{d/2}} \sum_{i \in I} |i\rangle (\sqrt{1-g(i)}|0\rangle + \sqrt{g(i)}|1\rangle) \quad (4)$$

ここで、関数 $g(i)$ は、中点近似の式 (2) と同じ定義を用いた。中点近似やモンテカルロ法では、アルゴリズムの計算コストは関数 $f(x)$ の呼び出し回数で数えられたのに対応して、量子アルゴリズムでは、式 (4) の演算の回数で数えられる。

式 (4) の演算後の状態の補助ビットを読み出したとき、1 となる確率は、期待値の中点近似 (2) の値 $S(f) = \frac{1}{m^d} \sum_{i \in I} g(i)$ で与えられる。このため、式 (4) の状態に対して、繰り返し測定を行って補助ビットが 1 になる確率を推定できれば、期待値の近似値が得られることとなる。ただし、単純に繰り返し測定を行った場合には、推定誤差 ϵ を達成するには、中心極限定理により $O(1/\epsilon^2)$ 程度とモンテカルロ法と同程度の計算コストを要することとなる。

この制限を回避し、量子コンピュータでよりよい推定誤差を達成するためのアルゴリズムとして振幅増幅法が知られている。補助ビットに 1 が得られる確率が p であるとしたとき、単純に j 回繰り返し測定をすると、1 が得られる確率はおおむね $j \times p$ 程度である。一方で、振幅増幅法を用いると、同じ j 程度のコストで 1 が得られる確率が $j^2 \times p$ 程度まで 2 乗加速することができることが知られている。この確率が増幅された状態を用いて、 p の推定を行うことで、計算コストを $O(1/\epsilon)$ 程度 (1/2 乗) に削減することが可能となる。

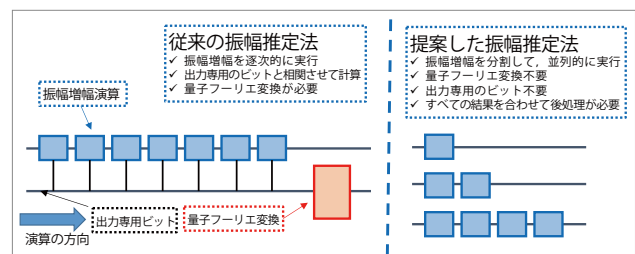
振幅増幅法では、振幅増幅回数 j を増やしていくに連れて、確率が増幅されるが、確率が 1 に到達した後にさらに振幅増幅を行うと、確率は j に対して振動を行う。確率を推定する振幅推定法では、従来、振幅増幅法に量子フーリエ変換を組み合わせ、この振動の振動数を求めることで $O(1/\epsilon)$ の計算コストの削減を達成していた。この振幅増幅法に量子フーリエ変換を組み合わせたアルゴリズムは非常に演算数が多く、現在の量子コンピュータでは、数

ビット程度 (1 次元を数分割程度) での検証しかできていない。量子コンピュータのハードウェア性能の向上により、いずれ、このアルゴリズムが利用できるようになるかと期待するが、少しでも早い量子コンピュータの活用に向けて、筆者らの研究グループでは、このアルゴリズムの改良を行ってきた。

前述のように、従来の振幅推定アルゴリズムは振幅増幅法と量子フーリエ変換の組合せであるが、計算コストの削減は振幅増幅法に由来しており、量子フーリエ変換は削減には寄与していない。したがって、筆者らの研究グループでは、量子フーリエ変換を使用しない新たなアルゴリズムを提案した (図-3)。提案したアルゴリズムでは、量子フーリエ変換を使用しないことで、制御ユニタリ演算と呼ばれる演算を大幅に削減することが可能となっている。具体的なアルゴリズムとしては、振幅増幅により、確率 p を変化させた状態の測定結果から、尤度関数を構成し、最尤推定により p を求めるという手法である。詳細については解説⁴⁾を参照されたい。

これに加えて、筆者らのグループでは提案アルゴリズムを実際に IBM の超電導量子コンピュータで実行し、現状のハードウェアにおいて、提案アルゴリズムの結果に、量子コンピュータのノイズがどのように影響するかを確認し、ノイズが多少あったとしてもアルゴリズムが動作するような改良を行った。さらに、ノイズがない場合には前述のアルゴリズムと同等の性能を示すが、ノイズがある場合には、より計算コストを下げられるような新たなアルゴリズムの提案も行っている。

この筆者らのグループのアルゴリズムでは、振幅増



■図-3 提案アルゴリズムの概念図

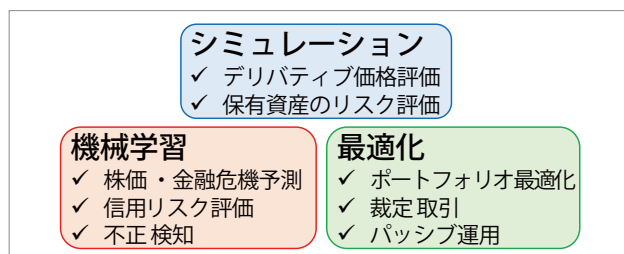
幅の具体的な回数の組を規定していなかったが、その後、ほかの研究グループから、厳密に計算コストを見積もれる振幅増幅回数組、高速化の程度は従来のものより劣るがより演算量が少ない振幅増幅回数組等、さまざまな方向性の研究が進められている。

最後に、念のために改めて強調しておくが、このようなアルゴリズム改良を行ったとしても、今後数年の量子コンピュータで、この期待値推定アルゴリズムが有用なタスクで動作する見込みはほとんどない。これは式(4)の演算を構成するための基本演算の個数が非常に多く、近い将来に実現されるノイズのある量子コンピュータでは正確な演算を行うことが困難なためである。ここで示したような研究により、アルゴリズムを実行するのに必要な量子コンピュータの性能要求(ノイズの大きさ等)を下げることにより、エラー訂正等に必要オーバーヘッドを少しでも減らし、活用時期を早めることに貢献できればと考えている。

デリバティブ価格評価以外の応用

ここまで、量子コンピュータの応用先として、将来の価格変動のシミュレーションによるデリバティブ価格評価について紹介したが、このほかにも多くの金融計算へのアプリケーションが提案されている(図-4)。特に、近い将来のノイズのある量子コンピュータであるNISQの活用に向けて、最適化問題や機械学習の量子アルゴリズムの応用が盛んに議論されている。

最適化問題とは、ある関数の値を、最大(または最小)にするような解を求める問題である。金融計



■図-4 適用先として検討されている問題

算では、最適な金融資産の組合せを見つけるポートフォリオ最適化、同一価値の商品の価格差を利用して利益を獲得する裁定取引、さまざまな金融商品を組み合わせて平均株価等と同様の値動きを行うパッシブ運用等、さまざまな最適化が行われている。これらの最適化では、計算資源の問題により、多くの場合に、制約条件や問題のサイズ等の簡素化した上で計算を行っており、これらの制限のない、より高速な最適化手法が求められている。

機械学習の量子アルゴリズムの詳細については御手洗氏の記事にあるが、これらを金融計算に、たとえば金融危機や株価の将来予測、信用リスク評価、不正検知等に適用するという研究も進められている。これらのNISQ向きのアルゴリズムの多くは、まだ、提案段階であり、小さなトイモデルでの検証が行われている状況である。今後より大規模な実データに対する検証が進められ、現実的なアプリケーションに利用できることを期待したい。

そのほかの研究の方向性としては、量子コンピュータの知識を活用した金融モデルの再構築の可能性も考えられる。金融のモデルは自然現象のモデルとは異なり、背景に強固な、再現性のある基本法則があるわけではなく、現実の現象をある程度説明するための単なるモデルとしての意味合いが強い。より量子コンピュータに適した新たな金融モデルの再構成という方向性にも期待したい。

参考文献

- 1) 金融市場における最新情報技術, 情報処理, Vol.53, No.9 (Sep. 2012).
- 2) Egger, D. J., et al.: Quantum Computing for Finance: State-of-the-Art and Future Prospects, IEEE Transactions on Quantum Engineering (2020).
- 3) ジョナル: フィナンシャルエンジニアリング[第9版]デリバティブ取引とリスク管理の総体系, 金融財政事情研究会(2016).
- 4) 宇野隼平: 量子コンピュータを用いた高速数値積分, みずほ情報総研技報, 10(1) (2019).

(2020年12月24日受付)

■宇野隼平 shumpei.uno@mizuho-ir.co.jp

名古屋大学大学院卒業, 博士(理学). 専門は素粒子物理学, 計算物理学. 2018年より, 慶應義塾大学量子コンピューティングセンターの共同研究員として, 金融分野への量子コンピュータの活用の研究に従事.

[面白いぞ量子技術]

5 量子コンピュータと量子化学計算

—量子コンピュータによって量子化学は恩恵を受けるのか?—

応
般

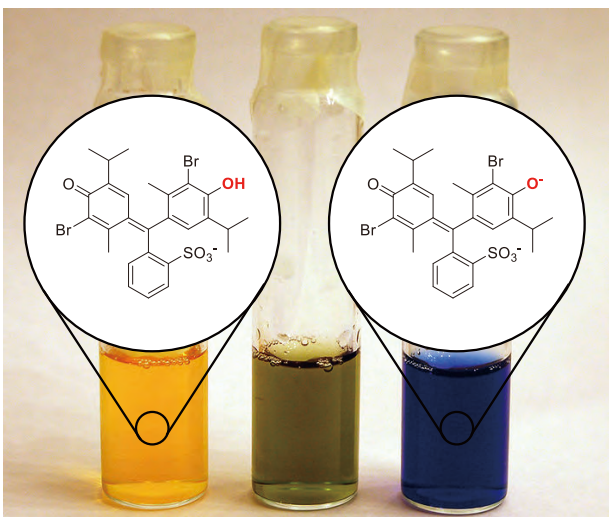
大西裕也

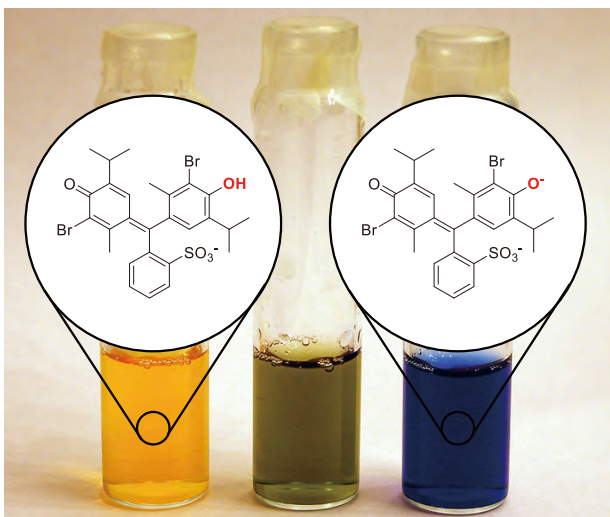
JSR (株)
RD テクノロジー・デジタル変革センター
マテリアルズ・インフォマティクス推進室

量子化学計算とは?

量子化学計算は何に使えるのか?

本稿では近い将来の量子コンピュータの活用先の1つとして有望視されている量子化学計算について、なるべく情報処理の専門家がその面白さや難しさを感じてもらえるように解説してみたいと思います。

本題に入る前に、量子化学計算が一体何に使えるのかについて簡単に触れておきます。量子化学計算は、誤解を恐れずにいえば、原子レベルの化学現象のシミュレーションの一種です。多くの方々がイメージする化学反応は、試験管の中の薬品に別の薬品を入れると色が変わるといったようなマクロな変化かと思えます。そのとき、試験管の中を分子レベルで観察すると、-1



■図-1 BTB 溶液による pH 変化の検出と BTB 分子構造の変化

のようにある分子が別の分子に変化して、元々吸っていた波長とは違う波長の光を吸うようになったという変化が起きています。反応はどうやって進むのか、どのような色に変化するのか、こういった分子レベルのミクロな現象を「シミュレーション」することができるものが量子化学計算です。量子化学計算はアカデミックのみならず製薬企業から石油産業や素材産業まで、すでに多くの場面で産業的にも活用されています。データ取得コストが実験に比べて低い場合が多く、材料の性能予測や構造提案を機械学習を用いて行うマテリアルズ・インフォマティクスと呼ばれる手法のためのデータ作成のためにも使われるようになっていきます。本稿では特に分子のための高精度量子化学計算について説明しますが、固体や表面であっても電子の分布を表現するための関数形が変わるだけで、高精度な計算結果を得ようとするときの本質的な難しさは変わりません。

高精度量子化学計算は何が大変なのか?

量子化学計算は原理的には微視的な化学現象を非常に高精度に予測することができます。それは、微視的なスケールでの化学現象の主役となる原子核と電子が従う方程式が分かっているからです。これは多くの場合 Schrödinger 方程式になります。ここでは以下の時間に依存しない Schrödinger 方程式を考えることにします。

$$\hat{H}\Psi = E\Psi \quad (1)$$

この式で \hat{H} は Hamiltonian と呼ばれる演算子で計算したい系を指定すると形が決まります。 Ψ と E はそれぞれその系の波動関数とエネルギーであり、これらは未知です。波動関数とは量子力学で系の状態を表す関数であり、これが分かるとその系がどのような量子力学的な性質を持っているかが分かります。ここでは Schrödinger 方程式について詳しく説明することは避けませんが、この式が固有方程式の形で表されるため、Hamiltonian を行列表示できれば、それを対角化することで固有関数と固有値としてそれぞれ波動関数とエネルギーが得られるのだということを納得してもらえればと思います。ただ、残念なことにはこの方程式を「厳密に」解くためには無限の計算リソースが必要になってしまいます。通常我々が興味がある Schrödinger 方程式の中の波動関数は分子の中の電子の確率振幅なのですが、これを「厳密に」表現するために無限次元の基底を用意する必要があるのです。それでは到底解けないので、現代の量子化学では物理的な性質に基づいた関数形をした有限の基底で近似をすることが多いです。有限の基底であっても、電子同士の多体相互作用を厳密に表現するためには電子数の増大に伴って指数関数的に大きくなる行列の固有値計算すなわち対角化が必要となり、実際に興味があるようなサイズの分子や表面・固体の計算は到底できません。そこで、さらに電子同士の相互作用も近似的に表現しています。つまりよく使われる量子化学計算では、[図-2](#) に示すように (1) 電子の確率振幅を表すための基底と、(2) 電子同士の相互作用を記述するための数式という2つの点で近似を導入しているのです。ここで、量子コンピュー

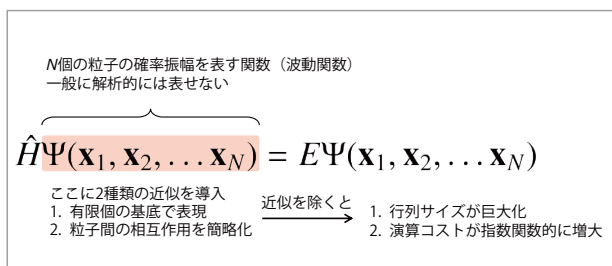
タが期待されているのは、(2) の近似を取り除きつつも計算リソースを低減できるのではないかと、という点です。この点については後の節で詳しく説明したいと思います。

実は、量子化学計算のプログラム作成はこれ以外にもいくつも大変な作業があります。量子コンピュータという本題からは少し外れますが、従来のノイマン型コンピュータ（以降古典コンピュータ）で量子化学者が取り組んできた計算上の苦勞と工夫をいくつか紹介したいと思います。

古典コンピュータでの量子化学計算の現状は？

量子化学計算の発展は HPC (High Performance Computing) 抜きには語れません。開発者たちはその時代の最先端のコンピュータをいかにして活用し、これまではできなかった計算を行うかということに腐心してきました。量子化学者たちの工夫の例としてまず、Obara-Saika のアルゴリズムを紹介します。

量子化学計算で比較的計算コストが高いステップに電子間反発積分というものの計算があります。古典的な見方に従えば、同じ負の電荷を持った電子と電子は距離の逆数に比例した位置エネルギーを持つことになりませんが、古典力学のように電子の位置を決めてエネルギーを計算することはできないので、確率振幅の積を全空間で積分することでこれを求めます。これが、電子間反発積分と呼ばれるゆえんです。前節で、電子の確率振幅は物理的な性質に基づいた関数で表現すると述べましたが、多くの量子化学計算では原子に中心を置いた複数のガウス型関数でこれを表現します。この積分を効率よく計算することは量子化学計算のパフォーマンスを向上させるために今でも重要なテーマです。プログラム上の困難を端的に言うと、工夫をせずに実装するとループ長の短いループが多段になってしまうキャッシュミスヒットが頻発することです。特に Obara-Saika の方法が考案された 1980 年台後半は Cray-2 や NEC SX-2 といったベクトル型のコンピュータが高い性能を発揮していた時代であり、これに対応する必要があったわけです。Obara と Saika はこの間



■ 図-2 Schrödinger 方程式と実際に解くために導入している近似の概要

題を解決するために数式上で前処理をする順番を工夫することで、ループ長が長くなるようなアルゴリズムを考案しました。その後ベクトル型コンピュータは主流でなくなるわけですが、現在再び SIMD 幅が大きなスカラ型コンピュータが主流になっていることで Obara-Saika の手法は依然として重要な手法となっています。

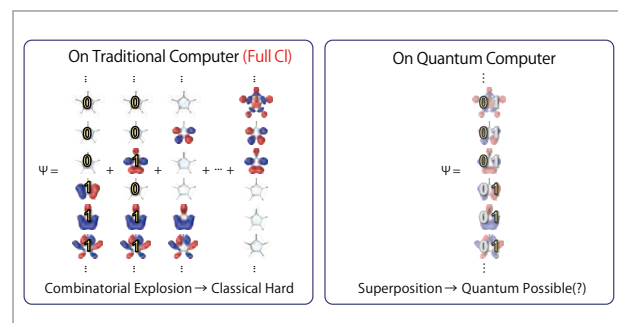
もう1つの例は並列コンピュータへの対応です。高精度な量子化学計算では非常に大きな行列(テンソル)の積を何度も計算することがあります。大きな分子では行列(テンソル)のサイズは数 TB を軽く超えることもあります。これをメモリにのせたまま計算できれば大きな分子の高精度計算が現実的な時間で可能となるため、開発者たちは巨大な行列積を複数のノードのメモリに分散させて計算する方法を開発してきました。米国の Pacific North National Laboratory では主に量子化学計算ソフトウェア向けに Global Arrays という区分化大域アドレス空間を活用したツールが 1996 年から開発されています。Global Arrays を用いることで、複数ノードにまたがったメモリ空間をプログラム上はあたかも 1 つの巨大な空間として取り扱うことができ、複数の巨大な配列をその都度 MPI で分散させるというようなことをしなくても済みます。これは計算したい分子によってサイズが異なる巨大な配列に対応しなければならないソフトウェアを書く上で、とても便利なツールでした。また分散されたテンソルの積を効率よいスケジューリングで実行するために Cyclops Tensor Framework というツールも 2011 年から開発されています。この Cyclops Tensor Framework は元々は高精度量子化学計算プログラムのために開発されたものですが、一般的な巨大なテンソル積に活用できるため、量子コンピュータのシミュレーションに必要なリソース推定にも活用されています。

ほかにも GPGPU のための混合精度演算であるとかガウス基底ではなく wavelet を用いる手法が提案されるなど、常に新しいハードウェアに適したアルゴリズムと実装が試みられており、依然としてパフォーマンスの向上が続いています。

量子コンピュータと量子化学計算

量子コンピュータに期待されていることは？

前章で触れたように量子コンピュータを用いると古典コンピュータではできなかったような量子化学計算が可能になると期待されています。なぜそれが可能かということを模式的に示したものが図-3 になります。現在主流の量子化学計算手法では、図の左のように 1 つの分子軌道に電子が 1 つ入っているという近似をします。ここで分子軌道は 1 つの電子の確率振幅を近似的に表現したものと考えてください。分子中のすべての電子の確率振幅(全電子波動関数)は、これら一電子分子軌道を要素とする Slater 行列式で表現されます。一電子分子軌道は、Fock 演算子と呼ばれる 1 つの電子の運動エネルギーと位置エネルギーを表現した演算子を用いた固有方程式の固有関数となるように反復計算を用いて決めます。したがってそれぞれの分子軌道は固有値を持つことになり、Hartree-Fock 法と呼ばれる近似手法では、エネルギーの小さいものから順に電子に占有されているものとします。ここで、なぜ図中で電子に占有されていない軌道が存在するのか疑問を抱いたでしょう。これは、この分子軌道をつくるためにさらに原子軌道と呼ばれる各原子に中心を置くガウス型関数を使い、その線形結合で分子軌道を作るからです。分子中の電子は複雑な分布をしているため、その分布(確率振幅)を表現するためには電子数よりも多くの原子軌道を必要とします。電子数よりも非常に多くの直交した原子軌道の線形結合で分子軌道を作るた



■図-3 古典コンピュータと量子コンピュータでの波動関数の表現方法の違い

め Hartree-Fock 法では電子が入っていない「空(から)の」分子軌道もできてしまいます。この空の分子軌道が高精度計算では計算コストの急速な増大を招きます。なぜならば Hartree-Fock で導入されている近似を取り除くために、図の左側に書いてあるように占有軌道から空の軌道に電子が移った「励起した」電子配置をすべて考えて全電子波動関数を表現する必要があるからです。

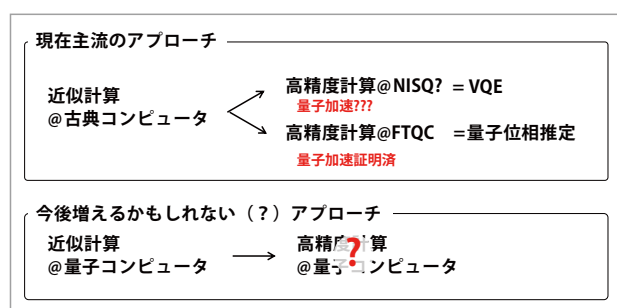
ここで計算に必要なリソースがどれくらい増えるか見ておきます。電子が入っていることを占有 (Occupied) と呼ぶので、その数を N_0 と書き、非占有 (Unoccupied) 軌道の数を N_U と書くこととします。高精度計算では $N_U > 10N_0$ くらいが必要となります。水分子を例にします。電子数が 10 なので $N_0=10$, $N_U=100$ として考えてみます。1つの電子配置のときは、その場合の数は 1通りです。占有軌道の1つの電子が空軌道に移動した(一電子が励起した)配置は、 ${}_{10}C_1 \times {}_{100}C_1=1,000$ 通りになり、それぞれの配置の重みを保存したければ要素数 1000 の一次元配列を用意すればよいので、倍精度実数で保存しても 8KB です。ところが五電子励起では ${}_{10}C_5 \times {}_{100}C_5=18,972,455,040$ 通りで 152TB が必要となってしまいます。思い出してもらいたいのは、これはたかだか 10 個の電子しか持っていない水分子の計算で各配置の重みを保存するためだけに必要な容量だということです。我々はもっと大きな分子の対角化をしたいので、これがいかに絶望的なタスクかということが分かるかと思います。もちろん、古典コンピュータ向けの高精度計算アルゴリズムは、この問題を回避するように、より少ない軌道数やより少ない電子励起の効果の取り込みで精度が出せるようにうまい近似が導入されており、水分子よりもかなり大きな分子の計算ができるわけですが、それでもやはり要求される計算リソースは分子サイズが大きくなるにつれて膨大になっていきます。

このような組合せ爆発がなぜ起こってしまったかというと、本来は占有か非占有か分からない軌道を古典コンピュータで表現するために無理やり占有 (1) か非占有 (0) に区別し、その場合の数をすべて考えるというこ

とをしたためです。では量子コンピュータではこれがどうなる(と期待されるか)というのが、図-3の右側です。占有を 1、非占有を 0 と表現したとき、量子ビットは 1 でもあり 0 でもある状態をとることができるので、軌道の数だけの量子ビットがあれば、すべての場合を表現できることになり、古典コンピュータ上で起こった組合せ爆発を避けることができます。

量子コンピュータでの量子化学計算の方法は?

旧来の量子化学計算を一部置き換える目的で盛んに研究されているアプローチは大きく 2 つが挙げられます。1 つは量子位相推定 (Quantum Phase Estimation, QPE) で、もう 1 つは変分的量子固有値解法 (Variational Quantum Eigensolver, VQE) です。後者に関しては訳語が定まっていないため、以降では広く使われている VQE という略称を使います。量子位相推定は量子加速が得られることが証明されているアルゴリズムですが、VQE に量子優位性があるかどうかはまだ知られていません。図-4 に示したようにしばしば、量子位相推定は誤り訂正付きの汎用型量子コンピュータ (Fault Tolerant Quantum Computer, FTQC) 向けで、VQE は近い将来のノイズがある中規模の量子 (Noisy Intermediate-Scale Quantum, NISQ) デバイス NISQ 向けと説明されます。量子位相推定には量子逆フーリエ変換が必要となるため多くのゲート操作が必要で、また倍精度実数程度の桁数を表現するために多くの量子ビットも必要となるため、FTQC が必要であることに間違いはありませんが、VQE が NISQ 向けかという点、近年のさまざまな実験や必要リソース推



■図-4 量子コンピュータでの量子化学計算に関するアプローチ

定を見る限りは個人的には NISQ で古典コンピュータを超えるような計算は難しいのではないかと考えています。なぜそう考えているかについては次節で述べたいと思います。

NISQ での難しさは？

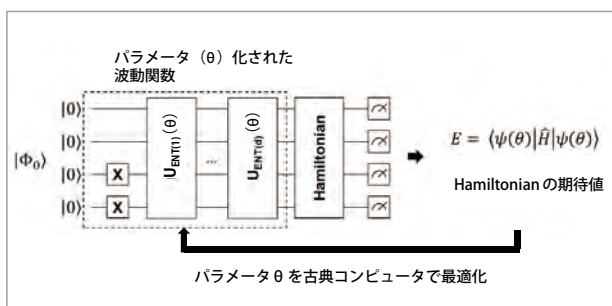
本節では NISQ での量子化学計算特有の難しさについて考えてみます。NISQ での問題は、やはり量子状態の寿命が限られるため置けるゲートの数に限界があるということです。

古典コンピュータでの高精度計算で組合せ爆発が起こるほど大量の電子配置を考えないといけないということは、複数の配置がそれなりの重みを持っているということを意味します。したがって、量子コンピュータ上でそれらの配置に相当する厳密な全電子波動関数を作成するためにも、[図-5](#) の UENT で表されている部分でかなり複雑なエンタングルメント状態を作り出す必要があります。そのようなエンタングルメント状態を作り出す方法として、現在 2 つの方向性が模索されています。1 つは Unitary Coupled-Cluster 法に代表される物理的な要請に基づく手法です。この方法の利点は、本来波動関数が満たすべき性質を数式の段階で考慮できている点ですが、計算上の弱点として、これを用いると数原子分子であっても数万個もの CNOT ゲートが必要になってしまうという点が挙げられます。もう 1 つの方法として、量子回路上でエンタングルメントを適当に作る方法があり、Hardware Efficient Ansatz や Heuristic Ansatz と呼ばれています。この方法だとゲート数は少なくなるのですが、まだまだ発展途上の

手法であり、よい初期値が分からなかったり、パラメータ空間での地形が分からなかったりしてパラメータの最適化が困難になるという問題があります。ここに、パラメータ化された量子回路で表される全電子波動関数が物理的要請に従わなくてはならない、という量子化学(量子力学)特有の問題があらわれてきます。物理的な要請を満たしながらも少ないゲート数で表現できる方法の確立が望まれます。

情報処理の観点からの問題解決方法として、物理に基づいたエンタングルメントの手法でのゲート数をコンパイラによって削減するという研究も行われており、英国の Cambridge Quantum Computing は `t|ket>` というフレームワークの開発を行っています。また、ゲート操作ではなくパルスを用いて相関波動関数を作成する ctrl-VQE という手法なども提案されており、今後も制御レベルからミドルウェア、ソフトウェア、アルゴリズムとすべての分野での発展が期待されます。

もう 1 つ大きな問題として、少ないゲート数であってもノイズによって測定結果が正しい分布にならないというものが挙げられます。量子化学計算で行いたいことの 1 つに複数の反応のエネルギーを算出し比較するというものがありますが、意味のある比較を行うにはかなりの精度が要求されます。たとえば、競合する 2 つの化学反応 (1) $A + B \rightarrow C$ と (2) $A + B \rightarrow D$ が考えられる場面で、生成物の比を計算で予測したいとしましょう。このとき、要求される計算精度は (1) の反応と (2) の反応のエネルギー変化の「差」で 1 kcal/mol のオーダーです。量子コンピュータによる計算結果のばらつき(エラーバー)がこのオーダーを超えてしまうくらい大きくなってしまえば、計算の意味がなくなってしまいます。このエラーバーを十分に小さくするためには測定を最低でも 10^6 回程度実行する必要がありますが、測定ノイズによって正しい期待値の分布が得られないとさらに膨大な数の測定が必要になってしまいます。特に 2020 年現在のようなクラウド型の量子計算機では一実験あたりの測定回数の上限が決められていることもあり、大きな分子で正しい期待値の



■ 図-5 VQEのスキーム

分布を求めるタスクはきわめて困難であると言えるでしょう。この量子化学計算に対するノイズ問題に対して、ミドルウェアの観点からはマシン固有のノイズを検知し、エラーの少ない量子ビットを使うようなコンパイラを作るという研究があり、この方向は今後も重要な技術になると考えられます。アルゴリズムとしてはエラー緩和や状態復元といった手法がすでに検討されており、一定の成果を見せています。

本節で述べたことは NISQ での難しさの一部分です。ほかにも深刻な問題として、パラメータ空間がほぼ平面でコスト関数の最適化が困難になる不毛な台地 (Barren plateau) 問題などは量子古典ハイブリッドアルゴリズム共通の問題として精力的に研究されています。このように VQE を用いて古典コンピュータではできないような分子の高精度計算を行う、というのはきわめて難しい問題なのではないかと筆者は考えています。仮に上記のような問題が解決されたのであれば、それはもはや NISQ ではなく FTQC に匹敵する性能のデバイスではないかと思われます。

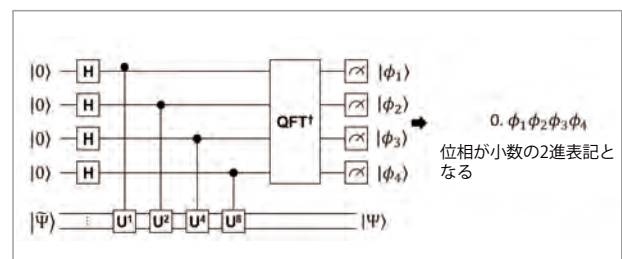
ただし、筆者は VQE そのものが無価値であると考えているわけではありません。このことと関係する FTQC であっても難しいことを次節で述べたいと思います。

FTQC でも難しいことは?

FTQC で有望視されているアルゴリズムは量子位相推定です。前々節でも述べたようにこれは FTQC を必要とするわけですが、FTQC ができれば古典コンピュータではできなかった計算がすぐにできるかという点が残念ながらそうではありません。量子位相推定は、ある試行関数を図-6の U_1 から U_8 などによって表されるゲートを作用させ時間発展させることで、Hamiltonian の固有値を取り出す手法です。したがって、ある試行関数が真の固有状態とはじめからある程度の重なりを持っている必要があります。ところが、我々があえて量子コンピュータを使って解きたいような問題では真の固有状態がどんな形をしているか分かりません。もしそれ

が分かるような問題であれば、それはエンタングルメントが少ないような計算対象なので、伝統的な量子化学計算を古典コンピュータで実行しても満足のいく結果が得られます。したがって FTQC でも難しい量子化学固有の問題として、十分に良い試行関数を作ることが挙げられます。この点に関してすでに多くの研究者が取り組んでいます。筆者は VQE によって作られるパラメータ化された波動関数が量子位相推定のための試行関数として使えるのではないかと考えています。VQE によってエネルギーが厳密に求められなかったとしても、試行関数としては伝統的な量子化学計算から得られるものよりも、ずっと量子コンピュータに適したものになるのではないかと期待しています。この点に関して、精度を保ちつつ回路を圧縮する問題などは情報処理の観点からも面白いのではないかと思います。

量子化学に限らず FTQC を用いて古典コンピュータではできないような計算をしようと思ったときに、ソフトウェア実装上で問題になるだろうと思われることが1つあります。それは古典コンピュータのメモリに載らないサイズの配列ができたときにどう対処するか、という問題です。現在の計算スキームでは、VQE であっても量子位相推定であっても試行関数や Hamiltonian を作成する際には古典コンピュータを使っており、量子コンピュータで必要になる配列はすべて古典コンピュータのメモリに一度に保存しています。今後量子ビット数が順調に増えた場合には、これらが古典コンピュータの記憶装置にのらない可能性があり現在のような実装では対応できません。実際の量子コンピュータでの計算ではこれを一度に保持しておく必要はなく、図-7で示すように必要に応じて古



■図-6 量子位相推定のスキーム

典コンピュータで一定のまとまりで計算し、量子コンピュータへ順次流し込んでいけばよいはずですが、かなり面倒な実装が必要になってくると想像されます。

量子コンピュータを古典コンピュータでは扱えないような巨大なヒルベルト空間を表現する機械として使いたいときには、それらの間で情報をエンコード/デコードするところをうまく実装する必要があると思われます。このあたりはプログラムの部品をモジュール化していき、やりとりを標準化することができて OpenMP でのディレクティブのように指示行を挿入するだけで解決できる問題なのか、それとも古典コンピュータと量子コンピュータで演算を行う部分を、ハードウェアのスペックに応じて、それぞれにどのタイミングでどのように振り分けるかを MPI のように陽に記述したプログラムを書くことになるのかは筆者には判断できかねますが、ぜひコミュニティで良い方法を見つけていただきたいと思っています。

量子コンピュータで量子化学は恩恵を受けるのか？

ここまで読まれた方は、量子コンピュータで量子化学計算は結局のところ大した恩恵を受けないのではないか、と感じられたかもしれません。この点に関して、

近似計算
@古典コンピュータ

高精度計算@NISQ? = VQE

高精度計算@FTQC = 量子位相推定

古典メモリに乗り切らない場合、古典→量子の一方ではなく量子の処理に合わせて古典から逐次供給するようなプログラムにする必要あり

■図-7 古典-量子の真にハイブリッドなプログラムに求められるスキーム

筆者は長期では楽観的な立場です。そもそも量子コンピュータでの量子化学計算が難しく見える理由は、古典コンピュータのために考えられた伝統的な量子化学計算のスキームを無理やりあてはめようとしている部分があるからではないかと感じています。1つの分子軌道に電子が入っているか入っていないかという考え方は古典コンピュータとは非常に相性が良い考え方であり、普段量子性をあまり感じないスケールに住む人間にとっても自然な考え方のように思われますし、実際に簡単な分子では成功を収めています。一方で、強相関係といわれる計算対象では、そのような見方が破綻することが分かっており、量子化学と物性物理の両方の分野が融合しながら新しい計算手法が開発されていっています。ここに量子コンピュータという量子力学を再現する情報処理装置が加わることで、決定論的ではなく、真に量子論的にミクロな自然現象を観察することができるようになるようにパラダイム自体が変革されるのではないかと楽観視しています。この点で量子化学は量子コンピュータの恩恵を大きく受けるだろうと考えています。そのような時代にあっては、ソフトウェア開発者も決定論的ではなく、確率論的に動作するプログラムを当たり前のようにデバッグしているでしょう。そのような未来が数十年のうちに到来することを願って本稿を終わりにしたいと思います。

(2020年12月29日受付)

■大西裕也 Yuuya_Oonishi@jsr.co.jp

JSR (株) RD テクノロジー・デジタル変革センター マテリアルズ・インフォマティクス推進室 次長、博士(工学)。専門は量子化学計算。現在は、MI 推進の管理業務の傍ら量子コンピュータ関連の業務にも従事。

[面白い量子技術]

6 量子計算は機械学習に使えるか

— 応一般 近未来／誤り耐性量子計算のための量子アルゴリズム —



御手洗光祐 | 大阪大学大学院基礎工学研究科

量子計算と機械学習

量子コンピュータとは、必ず0と1のどちらかの値をとる従来のビットとは異なり、同時に0でかつ1であるような「重ね合わせ状態」をとれる素子、量子ビットを用いる計算機である。大規模な量子コンピュータが実現すれば、従来の計算機—古典コンピューター—では困難な計算タスクである素因数分解を高速に解いたり、あるいは組合せ最適化問題の計算量スケールを緩和したりできる。

1990年代から本格的にスタートした量子アルゴリズムの研究は、最近さらに活発化している。そんな中、近年の機械学習の成功に触発されて、量子コンピュータによって機械学習を高速化するためのアルゴリズム開発も盛んになってきた。これらのアルゴリズムは量子機械学習アルゴリズムと呼ばれている。今日までにさまざまなものが提案されているが、量子機械学習アルゴリズムは主に、(1) 近未来に実現されると予想されている比較的小規模な量子コンピュータの使用を念頭に置いたもの、(2) 現在すでに商用機が販売されている量子アニーリング機を用いるもの、そして(3) 数十年後に実現されると考えられている、エラー耐性のある量子コンピュータを使うもの、の3種類に大別される。

このうち(3)に分類されるもののほとんどは、理論的な計算量スケールが明確に分かっており、それは従来コンピュータのアルゴリズムよりもよい。たとえば、

データ数 N に対して従来型では $\text{poly}(N)$ の時間がかかっていた計算を、適当な(必ずしも現実的かは明らかではない) 仮定のもとで、 $\text{poly}(\log N)$ 時間で解くアルゴリズムなどがある。一方で、(1)、(2)に分類されるアルゴリズムは、基本的にはヒューリスティックな手法であり、理論的な高速化の保証がないものがほとんどである。その代わり、近い将来に使える可能性があるという点で注目を集めている。

本稿では、これらのアルゴリズムについてその概要を解説する。

近未来の量子機械学習アルゴリズム

近未来量子コンピュータのパワー

近年量子計算に向けたハードウェアは目覚ましい発展を遂げている。つい—昨年には、Googleの研究グループが53個の超伝導量子ビットを備え、かつその操作の忠実度が~99%程度であるようなデバイスを作製し、「量子超越」を達成したと発表した。量子超越とは、ある特定の計算タスクについて、古典コンピュータの処理速度を量子コンピュータが上回ったということの意味する。実際、Googleの論文¹⁾では、53qubitの量子コンピュータを使って200秒で実行できるタスクが、スーパーコンピュータ Summit (2019年当時TOP500 1位)で1万年かかると主張されている。もちろん、その後IBMのグループから、もっと効率的な手法を使

特集 Special Feature

えば数日でできるだろう、と発表されるなど、本当にスーパーコンピュータに勝っているかどうかは議論が残るところであるものの、少なくともそれに迫る勢いであることは間違いない。これらのデバイスは総じて、雑音のある中規模量子デバイス (noisy intermediate-scale quantum) を縮めて NISQ (ニスク) デバイスと呼ばれる。

たかだか 53 個の量子ビットを並べるだけで、何千、何万個ものコアを持つスーパーコンピュータに迫れるのはなぜだろうか？ これを簡単に説明しよう。

量子コンピュータを構成する量子ビットは、必ず 0 と 1 のどちらかの値をとる古典的なビットとは異なり、同時に 0 でかつ 1 であるような「重ね合わせ状態」をとることができる。ただし、私たちが計算結果を確認しようと量子ビットを「見た」ときには、量子ビットは必ず 0 か 1 に収束する。この収束先は確率的に決まる。具体的には、重ね合わせ状態の中にある 0 と 1 はそれぞれ複素数 c_0 , c_1 で表される重みを持っており、それぞれ $|c_0|^2$, $|c_1|^2$ の確率で 0 または 1 に収束することになる (図-1 (a))。

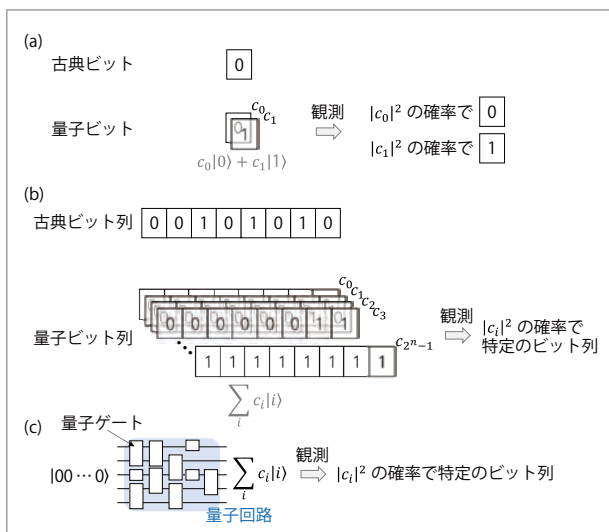
量子ビットが 1 つしかなければ、 c_0 , c_1 を保持しておくことによって、古典コンピュータでも簡単にその動き

を模倣できる。 $|c_0|^2$, $|c_1|^2$ の確率で 0・1 をサンプルすればよいだけだ。しかし量子ビット数が増えていくと、保持しなければならない複素数の数は指数関数的に増えていく。 n 個の量子ビットがあれば、一般に 000...0 から 111...1 まで、 2^n 通りの状態の重ね合わせが許され、その動きを厳密に模倣するならば $c_0 \sim c_{2^n-1}$ までの 2^n 個の複素数を使わなくてはならないからだ (図-1 (b))。このために、50 量子ビットあるだけで、単精度浮動小数点を使ったとしても $8 \times 2^{50} \text{B} \approx 8 \text{PB}$ もの記憶容量が必要となってしまふ。これがたかだか 53 量子ビットのデバイスでも、スーパーコンピュータを超えられるゆえんである。古典コンピュータにとって「量子コンピュータの動きを厳密に模倣しなさい」というタスクは、量子ビット数が大きくなるにつれて事実上不可能となる。このような能力を何らかの形で機械学習へと応用しようと、さまざまな研究が進められている。

NISQ デバイスに向けた機械学習アルゴリズム 量子状態を特徴量空間として利用する

量子機械学習の 1 つの方向性は、上記のような膨大な数の複素数を、特徴量の保存に使おうというものだ。特徴量とは、得られたデータ x の「特徴」を表すために作られる量のことをいう。この概念図を図-2 に示した。図-2 の円形のデータを、赤と青の点に分類するという機械学習タスクを考えよう。データを平面 (この場合は直線) で分割するのが最も簡単な分類アルゴリズムであるが、このデータはそのままではそのような線形分離は不可能である。しかし、図-2 の右のように、 $x_1^2 + x_2^2$ の軸を追加すれば、この 3 次元空間では簡単に線形分離することが可能となる。このように、あるデータ x に対して適当な変換を作用させ、高次元空間 (特徴量空間) へと移すことで、学習が簡単になることがある。

そこで NISQ デバイスが自然に持っている高次元空間を、この特徴量の保存に使おうというアイデアが考えられた。図-2 下のように、あるデータ x を n 量子ビットの量子状態へと、適当な量子回路 $V(x)$ を用いて埋



■ 図-1 (a), (b) 古典ビットと量子ビットの違いの概念図。(c) 量子回路図。各横線が 1 つの量子ビットを表す。論理ゲートの量子版である量子ゲートが左から順に初期化された状態 $|00 \dots 0\rangle$ に作用し、最終的に重ね合わせ状態 $\sum_i c_i |i\rangle$ が生成される。

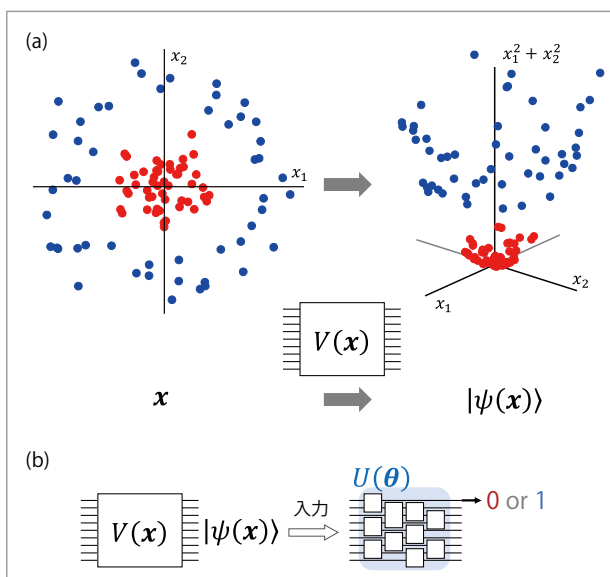
特集
Special Feature

め込む。すると x は 2^n 次元の空間に移されるが、その空間で機械学習を行おうというのである。例として、図-2 (b) のような方式がある。この方式ではまず、量子回路 $V(x)$ によってデータ x を量子状態 $|\psi(x)\rangle$ に埋め込む。その後、その状態をそのまま別の量子回路 $U(\theta)$ に通し、最終的に出力として1番上の量子ビットの0・1で分類を行う。このとき、 $U(\theta)$ には調節可能なパラメータ θ を入れておき、出力が正しい分類値を返すように、このパラメータ θ を最適化していく。このようにして「訓練」された量子回路は、NISQ デバイスの高次元空間に保存された特徴量をうまく選び出し、分類に役立てられることが予想できる²⁾。

実際に図-2 のようなとても初歩的な分類問題では、このアプローチがうまくいくことは確かめられているものの、手書き文字の分類のようなタスクについてうまくいくかどうかはまだ確かめられておらず、今後の検証が望まれている。

量子状態の確率分布を利用する

先にも述べたように、NISQ デバイス上に作られた量子状態からのサンプリングを古典コンピュータで模倣



■ 図-2 (a) 特徴量の概念図。(上) 円形のデータに対して $x_1^2 + x_2^2$ の軸を付加することで、線形分離可能となる例。(下) データ x を 2^n 個の複素数を持つ量子状態 $|\psi(x)\rangle = c_0(x)|00\dots 0\rangle + c_{2^n-1}(x)|11\dots 1\rangle$ に埋め込む。(b) 量子状態に埋め込まれた特徴量を使った機械学習の一手法。

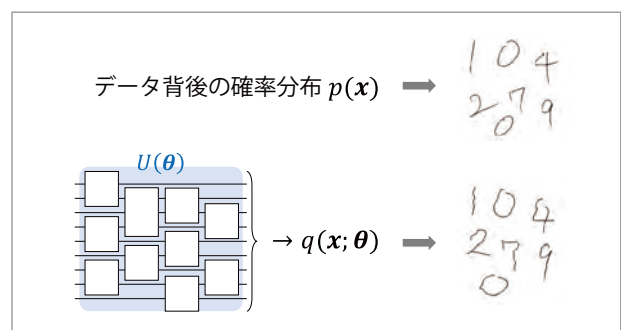
することは、量子ビット数が十分大きいとき非常に困難である。逆に言えば、NISQ デバイスのような量子的なハードウェアを用いない限りサンプリングが難しい確率分布が存在する。

そこで考えられるのが、その確率分布自体を直接機械学習に使うアプローチである。最も愚直なアプローチとしては、生成モデルへの利用が挙げられる。生成モデルとは、与えられたデータセット $\{x_i\}$ がある確率分布 $p(x)$ から生成されたものと考え、この確率分布 $p(x)$ とよく近似する他の確率分布 $q(x)$ のことを言う。この確率分布 $q(x)$ の構成に、NISQ デバイスでしか出力できない確率分布を利用してやろうというわけだ。図-3 にその概念図を示した。最近では、敵対的生成ネットワーク (generative adversarial network) など、もっと高度な機械学習モデルにこの考え方を応用しようという動きも出てきている。このあたりの動向は、文献3) に詳しい。

このアプローチも先の例と同様に、実際にはまだまだ非常に初歩的なデモンストレーションにとどまっているが、活発に研究が進められており、少しずつ大規模なデモンストレーションが行われていくだろうと予想される。

量子アニーリングを用いる量子機械学習

量子アニーラとは、ある特定の組合せ最適化問題を解くことに特化した量子デバイスのことを言う。動作方式も、図-1 (b) のように量子ビットを量子ゲートによって逐次的に操作していく方式とはまったく異なる。日本



■ 図-3 量子回路による生成モデル構成の概念図。パラメータ付き量子回路を使って生成した確率分布 $q(x; \theta)$ を、 θ の調整によってデータの背後にある確率分布 $p(x)$ に近づけていく。

特集

Special Feature

では、これらはアニーリング型/ゲート型量子コンピュータと呼ばれ区別されている。特化マシンであるが故、ゲート型よりも量子ビット数を増やすのが容易であり、すでに1,000量子ビットを超えるデバイスがD-wave社より発売されている。

量子アニーリングは、「0か1のどちらかを取る変数 s_0, \dots, s_n について、 $E(s) = \sum_i h_i s_i + \sum_{ij} J_{ij} s_i s_j$ という関数が最小値を取るような s_i の組を見つけよ」という最適化問題を解くことに特化したデバイスである。もちろん $E(s)$ を最小化する最適解が、量子アニーラを走らせるたびに毎回得られることが理想だ。しかし実際にはそうっておらず、近似的に $p(s) = e^{-\beta E(s)} / \sum_s e^{-\beta E(s)}$ という確率分布からビット列 s がサンプリングされているとみなせるようなのだ⁴⁾。ここで β はデバイスやその他の条件によって決まる定数である。

最適解が得られなくなってしまうのだから、これは最適化問題を解くという観点から見ると悲しいことだ。しかし一方で、一般に $e^{-\beta E(s)} / \sum_s e^{-\beta E(s)}$ という確率分布からのサンプリングは、実は通常のコンピュータにとっては難しいタスクであることが知られている。さらに良いことに、この確率分布からのサンプリングを使えば嬉しい機械学習アルゴリズムが存在する。ボルツマンマシンと呼ばれるニューラルネットワークの一種である。この機械学習モデルは、 $e^{-\beta E(s)} / \sum_s e^{-\beta E(s)}$ 型の確率分布を用いて学習・推論を行うものであり、まさにこの確率分布からのサンプリングが必須となる。そこで近年、量子アニーリングの出力をボルツマンマシンと対応付け、機械学習へと応用しようという研究が行われている。この方向性では、すでに多数の量子ビットを使えるという量子アニーリングの特長を活かし、NISQデバイスよりも大規模なデータセットを使った検証が進んでいる⁴⁾。

長期的な応用を見据えたアルゴリズム

誤り耐性量子コンピュータ

量子ビットは外界からの影響を非常に受けやすく、

放っておくとすぐに量子的な重ね合わせ状態が壊れてしまう。たとえばGoogleの量子超越実験で使われた超伝導量子ビットでは、 $10\mu\text{s}$ 程度で重ね合わせ状態が失われてしまう。1回の量子ゲート操作にかかる時間は10ns程度なので、まともに使えるゲート数は1,000回程度である。一方で、理論的に高速化が保証された最初のアプリケーションとして期待される量子化学ですら、 10^{10} 回程度の量子ゲート操作が必要と見積もられている。ハードウェアの進歩のみで、そのようなアプリケーションを実行できるようになるのは非常に難しいと考えられる。

より現実的なアプローチは、計算中に起こったエラーを逐次検出・訂正しながら計算を進めていく方式である。量子コンピュータにおけるエラー検出・訂正技術は量子誤り訂正と呼ばれており、この技術によってエラーが抑制された量子計算を誤り耐性量子計算という。そのアイデアは古典的なビット列の誤り訂正と同様で、1つの量子ビットの情報を、多数の量子ビットを使って冗長化しておくというものである。しかし量子誤り訂正に必要なオーバーヘッドは膨大である。たとえば100量子ビット相当の誤り耐性量子計算を行うには、物理的に100万個程度の量子ビットを用意する必要があるだろうと予想されている。

今現在の最先端ハードウェアは、Googleの研究グループが作製した50量子ビット程度のデバイスであり、誤り耐性量子計算の実現には程遠い。しかしこの誤り耐性量子計算を使えば、量子コンピュータは素因数分解や量子化学計算等の領域で古典コンピュータを超えると見積もられており、この計算能力が機械学習にも適用可能であるか研究することは長期的に意義があるだろう。以下ではこのような研究について紹介する。詳細に興味を持った読者には、文献5)をおすすめする。

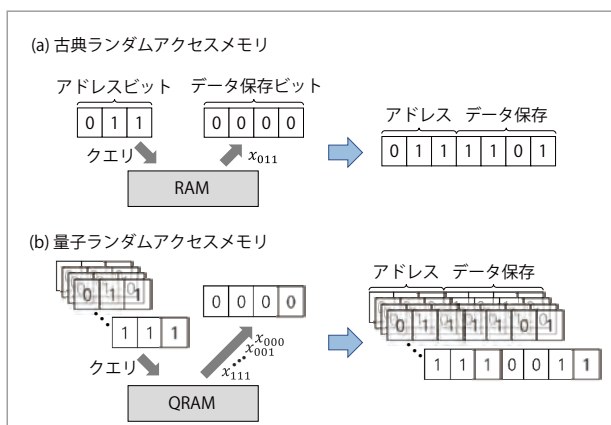
量子行列計算による機械学習

2009年にHarrow, Hassidim, Lloydらによって、正方行列 A 、ベクトル b に関する線形連立方程式 $Av=b$ の解 $v=A^{-1}b$ を、行列の次元 N について

特集 Special Feature

poly($\log N$) 時間で求める量子アルゴリズム (HHL アルゴリズム) が提案された。現在ではより一般に、行列 A の適当な関数 $f(A)$ をベクトル b に作用させるアルゴリズムが開発されている。このような行列操作は機械学習でも頻出であり、さまざまな応用先がある。たとえば、最も単純な機械学習モデルの1つである線形回帰、また有名な分類アルゴリズムであるサポートベクタマシンなどは、(擬似) 逆行列計算によって学習を行う手法だ。HHL アルゴリズムの提案以降、これらの機械学習アルゴリズムへの理論的拡張が進められてきた。これらはどれも指数的加速をうたうもの、すなわち古典コンピュータでは N について多項式時間かかっていたものを、poly($\log N$) の計算量オーダーへと落とすという提案である。

指数加速と聞くと大きな期待を持ってしまうが、これらのアルゴリズムが具体的な適用にはシビアな条件がつく。与えられたデータセット $\{x_i\}$ を、重ね合わせの形で効率的に量子コンピュータへと送ることができる、という条件だ。というのも、線形回帰やサポートベクタマシンで現れる行列の次元 N はデータの個数と等しいので、もしデータセットを量子コンピュータへと送るだけで $O(N)$ の時間がかかってしまったら、せっかくの指数加速が打ち消されてしまう。しかも普通に考えると、 N 個のデータの送信に $O(N)$ の時間が必要になるのは避けようがないように思える。



■ 図-4 古典/量子ランダムアクセスメモリの違い。QRAM はアドレスとして重ね合わされたビット列も受け付け、その重ね合わせを保ったままデータ保存ビットへとデータを送り込む。

そこで登場するのが、量子ランダムアクセスメモリ (QRAM) と呼ばれる機構である (図-4)。これはランダムアクセスメモリ (RAM) の量子版で、量子的に重ね合わされたアドレスを受け取り、その重ね合わせ状態を壊すことなく、各アドレスに対応したデータを返せるようなデバイスだ。このようなデバイスがあれば、データの保存されているアドレスを重ね合わせた状態を送り、 N 個のデータを一度の間合せで得ることができる。データ数に関する加速を目指す量子機械学習アルゴリズムには、QRAM の使用がほぼ必須である。しかしながら、QRAM はそのアーキテクチャの理論提案こそいくらかあるものの、量子誤り訂正のようにこれなら間違いなくできる、というコンセンサスが取れた構成がいまだに得られていない。いわゆるビッグデータの機械学習を考えると、量子コンピュータでデータ数に対する加速が得られるならば非常にインパクトが大きいが、上記のような事情によってこの方向性ではいまだ理論的にも実現の目処が立っていないのが実情である。

その他の量子機械学習手法

データ数に関する加速を目指す場合、QRAM の問題がついてまわるが、逆に言えば、それ以外の方向での加速であれば QRAM は問題とならない。そのようなものの例として、量子振幅推定と呼ばれるテクニックを基礎とする量子機械学習アルゴリズムがある。量子振幅推定は、適当な確率分布からのサンプリングが必要となるアルゴリズムの計算量オーダーを広く改善できる手法である。普通、サンプリングによって何らかの量を求めるとき、その統計誤差は通常サンプル数 M に対して $O(1/\sqrt{M})$ でスケールするが、この量子振幅推定アルゴリズムを使うと誤差のスケールを $O(1/M)$ に改善できる。具体的な例としては、ベイジアンネットワークの加速などがある。

量子インスパイアアルゴリズム

最後になったが、量子コンピュータの一応用先として研究されている量子機械学習が、実は最近古典的な機

機械学習アルゴリズムの高速化に寄与したことに触れておきたい。2018年に、当時最も注目されていた量子機械学習アルゴリズムの1つが、Ewin Tang という当時18歳の学生によって「脱量子化 (dequantize)」されたのだ⁶⁾。この量子アルゴリズムはHHLアルゴリズムの派生型を基礎として使うことで、指数的な高速化を達成すると考えられていたが、彼女によってそのような高速化が古典コンピュータのみでも可能であることが示された。その古典アルゴリズムの詳細な計算量スケールはかなり悪く、実用的であるかどうかは不透明なのだが、それでも指数的な高速化のインパクトは大きい。量子機械学習に限らず、今後このように量子アルゴリズムを「脱量子化」する、量子インスパイアアルゴリズムの研究が進むかもしれない。

量子機械学習の展望

本稿では、量子計算の原理にも触れながら、近未来の、あるいは長期的な応用を目指した量子機械学習アルゴリズム研究の現状について概観した。この分野は比較的新しい研究分野であり、大きな量子コンピュータができたとき本当に役に立つのかすら不透明な状況だと言えると思う。NISQデバイス向けのアルゴリズムであれば、もう少し大きなスケールのデータセットでの検証を待つ必要があるし、長期的なアルゴリズムでデータ数に対する加速を目指すのであれば、データと量子

コンピュータのインタフェースを真剣に考える必要がある。量子インスパイアアルゴリズムについても、実用性の検討が望まれる。

幸いなことに、ここ2、3年で、量子コンピュータのアプリケーション分野の研究開発人口は急増している。量子コンピュータのソフトウェアに主眼を置いたスタートアップ/ベンチャー企業も多くなってきた。筆者も2018年からQunaSysという量子ソフトウェアスタートアップの創業にかかわっている。これらの企業から次々に量子ソフトウェアパッケージが打ち出されており、特にNISQに関しては参入障壁も低くなってきているのではないだろうか。研究開発人口がさらに増えることで、量子機械学習、ひいては量子アルゴリズム全体の研究開発がさらに加速されることを期待したい。

参考文献

- 1) Arute, F. et al. : Nature, 574, 505 (2019).
- 2) Mitarai, K. et al. : Phys. Rev. A, 98, 032309 (2018).
- 3) Cerezo, M. et al., arXiv:2012.09265 (2020).
- 4) Benedetti, M. et al. : Phys. Rev. A, 94, 022308 (2016).
- 5) Schuld, M. and Petruccione, F. : Supervised Learning with Quantum Computers, Springer (2018).
- 6) Tang, E. : arXiv: 1807.04271 (2018).

(2020年12月25日受付)

■御手洗光祐 mitarai@qc.ee.osaka-u.ac.jp

2020年大阪大学大学院基礎工学研究科博士課程修了。博士(工学)。同年より同研究科助教・JST さきがけ研究者・(株) QunaSys CSO を兼任。



[面白い量子技術]

7 ダイヤモンド量子センサの可能性

—ピンクダイヤモンドが 高感度なセンサに—

応
般

波多野睦子 | 東京工業大学工学院

ニューノーマルでの ダイヤモンド量子センサへの期待

コロナ禍で急速に普及したオンラインでの講義や会議のハンゴに、そろそろ限界を感じている。集中力が散漫になり、妙な疲れが蓄積していく。何よりも相手の「オーラ」や「本音」を掴み切れず、それがまたストレスとなる。人に届くまでは情報は高速に通信されているが、それから先の脳に届くまではきわめてアナログ・低速であり、さらに脳における情報処理機構の全約はまだ明らかになっていないことも原因の1つであろうか。

ニューノーマルでは、より人間が重視され、人間の行動や心の変化が技術革新をリードする時代になるに違いない。視覚と聴覚だけでなく、触覚、臭覚、味覚、さらにはそれを司る脳や心のモニタが必要になり、高精度かつ非侵襲で計測できる高度なセンサの進化が重要となる。

本誌 (Vol.59, No.1 (2018)) の特集「脳情報科学が拓く AI と ICT」において、脳機能の解明が ICT 社会にとって役に立つ技術と認識されるようになり、さらに広い分野の科学の相互作用の進化の重要性が指摘されている。特に多くの人間情報を収集して解析するために必要な、実環境で使える BMI (Brain Machine Interface: 脳とコンピュータなどの機器とのインタフェース) の発展が不可欠と論じられている。

本稿で紹介するダイヤモンド量子センサは、量子力学的効果を利用して感度や分解能を物理法則の極限まで高められる次世代センサとして注目され、世界中で研究開発が活発化している^{1), 2)}。まだ基礎研究の段階にあるが、先述のニーズを実現できる可能性がある。

本稿では、ダイヤモンド量子センサの可能性を中心に、その原理、人工的に作製する技術、量子プロトコルを用いた計測、および応用の一部を紹介する。

量子センサのカギとなるのは、NV センタ (炭素を置換した窒素 (N) と隣接位置の空孔 (V) との複合欠陥) である。後述するが、熱的にも機械的にも安定なダイヤモンド結晶に閉じ込められているという特異な状態のため、NV センタの電子スピンは広い温度範囲で安定した振る舞いを示し、量子状態が長く維持される。したがって、さまざまなアプリケーションが期待される。さらに計測対象の範囲は広く、ナノからマクロスケールまでの空間分解能の磁場・温度・電場・圧力センサとして機能する。

図-1 に横軸に空間分解能、縦軸に磁気感度を取り、磁場センサとしての応用例を示す。蛋白質や生体分子の構造解析に必要なナノメータ領域、ドラッグデリバリーや免疫検査に適用される細胞計測に必要なミクロンの領域、生体・自動車・構造物の非侵襲計測に必要なミクロン以上の領域まで、空間分解能に対してスケーラブルな応用が拓ける。

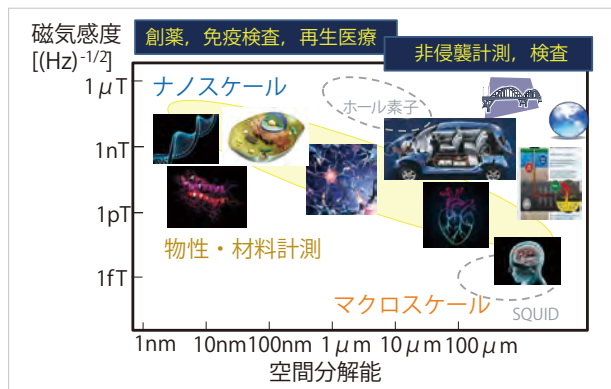
表-1 にダイヤモンド量子センサの特徴を、超伝導量子

特集 Special Feature

干渉計, 光ポンピング原子磁気センサと比較して示す。ダイヤモンドセンサは, 以下の他のセンサにない特長がある。

- 広い温度範囲, かつ大気中で動作
- 拡張性が高く, チップ化やアレイ化, 集積化が容易なため, より高度なデバイスが実現可能
- イメージングができ, NV 軸方位を利用したベクトル磁場を検出
- 代表的な微弱磁気信号であり, NMR (核磁気共鳴) 計測で計測対象となる, AC の核磁化信号も, 脳磁・神経等の DC の生体磁気信号も計測可能
- 飽和性が実用的になくダイナミックレンジが広い
- 個々の NV センタがナノスケールのセンサとして動作
- 情報 (磁場・電流) とエネルギー (温度) の同時計測

これらの特長を活かせば, システムの小型モ



■ 図-1 空間分解能と磁気感度から見たダイヤモンド固体量子センサの応用の可能性

■ 表-1 高感度な量子センサのベンチマーク

性能/機能	超伝導量子干渉計	光ポンピング原子磁気センサ	固体量子センサ	優位性
動作環境	極低温要	高温 (>100℃) 要	mk-600K の広範囲で動作可能	耐環境性
状態	固体 (超伝導体)	気体 (アルカリ金属蒸気セル)	固体 (ダイヤモンドや SiC)	全電気, チップ化, アレイ・積層化
イメージング	単体では不可	単体では不可	可能	ベクトルイメージング
感度 [$\sqrt{\text{Hz}}$]	<10fT	<1fT	~ pT	高感度向上が重要
ダイナミックレンジ	飽和性あり	飽和性あり	飽和性なし	
空間分解能	mm 以上	mm 以上	nm ~ mm	スケーラブル (nm ~ mm)
温度計測	不可	不可	可	エネルギー (温度) と情報 (磁場, 電流) の同時計測

ジュール化を実現するほか, 表-1 に示したような従来の磁気センサ単体では不可能であったベクトル磁場計測により, 神経ネットワーク内の信号の発生と伝播の方向性, 外部刺激に対する脳内反応の経路が解析できるようになり, 脳内, 特に脳深部の神経電流の分布を推定する精度が向上する。細胞から生体までの階層的でスケーラブルな計測結果とあわせ, 脳機能のダイナミクスを脳磁図から解析可能となる事が期待される。さらに磁場と温度の計測により, 情報伝達と活性化度の両方が同時に取得できる従来にはないセンサシステムを創出することができる。

ダイヤモンド中の量子ビット NV センタ

ダイヤモンドは, 炭素原子が正四面体状に完全に規則的に並びお互いに結合の手をつなぐことで非常に強く結びついている。ダイヤモンドが最も硬い宝石たるゆえんである。

NV センタは, その結晶の完全性を崩す構造的欠陥 (図-2 (a)) であるが, 赤色の蛍光を示し (図-2 (b)), 宝石としての価値が高まるとともに, 室内光中でもピンク色を示すいわゆるピンクダイヤモンドとなる (ピンクダイヤモンドは天然にも存在するが希少であり, 宝石的価値が高い)。そして, 量子センサとして科学的な価値が高まる。

NV センタは, バンドギャップの大きなダイヤモンドの深い準位にあることに起因して, 室温・大気下でも

特集
Special Feature

優れたスピコヒーレンス性を持ち、量子状態の初期化（偏極）と読み出し（検出）を光で行えるという稀有な特長を備えている。

さらに NV センタの電子スピン状態を量子的に精密に制御・観測することで高感度化が図れる。パルス磁気共鳴法を用いて、マイクロ波やラジオ波のパルス列を印加することで、スピンを操作することにより、デコヒーレンスを抑制するだけでなく、スピン間の量子効果を利用した検出感度の向上も可能である。

NV センタの形成方法としては、ダイヤモンド結晶中への窒素イオン注入、窒素を含むダイヤモンドに電子や陽子などの量子線照射を行う方法、あるいはマイクロ波プラズマ化学気相成長（CVD）法によるダイヤモンド膜合成中に NV センタを形成する方法、などが用いられている。

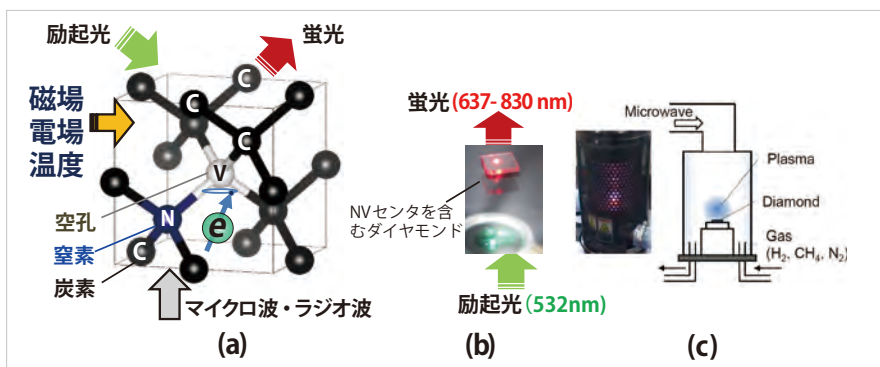
CVD 法においては、メタンと水素の混合ガスを

プラズマで分解することでダイヤモンドが合成される。さらに合成中に少量の窒素ガスを混合することで、ダイヤモンド膜中に NV センタが形成される（図-2 (c)）。CVD 法の長所は N-V 軸（N 原子から見た空孔（Vacancy）の方位で、炭素結晶内に 4 方位が存在し得る）の配向制御であり、アンサンブル NV センタを用いた感度向上に有効である。

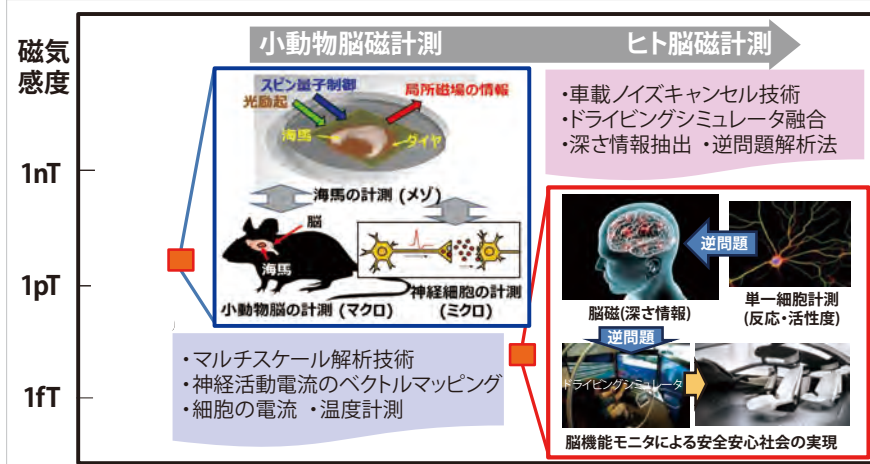
ダイヤモンド量子センサのターゲットと原理検証実験

量子センサの他のセンサにない特徴として、生体親和性が優れていること、また堅牢で広い温度範囲（mK ~ 600K）でも安定であることが挙げられる。これより応用として特に生体計測、およびエネルギーデバイスのモニタリングが注目されている。

前者は図-3 に示すように、小動物の脳磁→ヒト



■ 図-2 高感度センサになるダイヤモンド中の窒素-空孔複合体（NV センタ）
(a) 構造, (b) 磁場, 電場, 温度を赤色の蛍光変化で検出, (c) ダイヤモンドの合成方法：高密度プラズマによる化学気相成長法（CVD）



■ 図-3 生体計測への応用

特集 Special Feature

の脳磁のスケラブルな計測をターゲットとする。材料・デバイス・量子プロトコルによる高感度化に加え、断熱距離が不要で頭蓋に密着可能なこと、ベクトルイメージングが可能な利点も活かして、より高感度・高機能な計測実現が期待できる。

脳磁計測においては頭蓋外部で計測される磁場から頭部内部の神経の活動を推定する逆問題を解く必要があり、そのためには脳内組織や神経細胞の活動の理解とモデル化が不可欠である。単一神経細胞内信号計測、神経ネットワークの活性化度の計測、脳磁図計測を連携させた階層的研究の各階層におけるNVセンタの寄与により、逆問題解析のモデル精度を向上可能である。

脳磁計測の用途としては医療応用のみでなく、ヘルスケアや安全運転のための運転者のモニタも期待されている。実際の適用には、アクティブシールドを含め、磁気ノイズと脳磁信号の分離とノイズキャンセリングを行う技術も開発する必要がある。

ダイヤモンド量子センサの応用先として注目されているもう1つの分野がエネルギーデバイスのモニタリングである。エネルギーデバイスは一般にナノからマイクロスケールのパワーデバイス、マクロスケールのパワーエレクトロニクス機器、電池などから構成され、全体の高信頼化・高性能化には各レベルでのスケラブルなモニタリングが重要である(図-4)。

パワーデバイス、パワーエレクトロニクス機器に

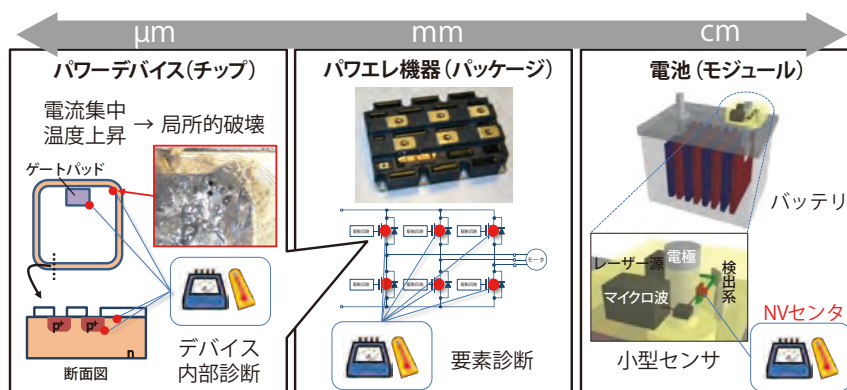
は、故障・破壊リスク予測のための局所電界、温度、電流の評価が重要である。ダイヤモンドパワーデバイスの内部診断にはNVセンタを、炭化ケイ素(SiC)パワーデバイスにおいてはシリコン空孔(VSi)をセンサとして利用する。

電池システムとしては、現行のEV車の電池モニタに使用されている電流センサの精度は1A程度である。これを10mAまで向上できると、電池の充放電電流の計測精度が向上し、その積算値としての電池残量予測精度が向上する。これにより、電池容量24kWhのEVにおける実質走行可能距離の約10%の向上が期待できる。そのため、車載の高雑音環境下でも大電流から微弱電流までの広いダイナミックレンジを測定でき、かつ電流・温度を同時に計測できるセンサが必要とされている。

ダイヤモンド量子センサは、現時点は可能性を検証している段階であり、社会や人へ役立つように進化させるには、物理、材料、デバイス、回路、システム、情報のレイヤ間の連携や異分野の融合を進めなければならないと考えている。本会での研究との連携を期待し、筆者らが取り組んでいる原理検証実験の例を紹介したい。図-5にその概要を示す。

(1) ナノスケールの核磁気共鳴(NMR)計測

核磁気共鳴(NMR)計測は、静磁場中では物質中の核スピンのエネルギー準位がわずかに分裂(Zeeman分裂)するため、分裂の大きさに対応した周波数のAC電磁波の共鳴吸収が生じることを



■図-4 エネルギーデバイス(電池、パワーデバイス)モニタリングへの応用

特集
Special Feature

利用し、物質の分析を行う技術である。AC電磁波の計測をコイルなどで行う現行のNMRでは、計測対象に 10^{13} 程度のスピンの必要である。

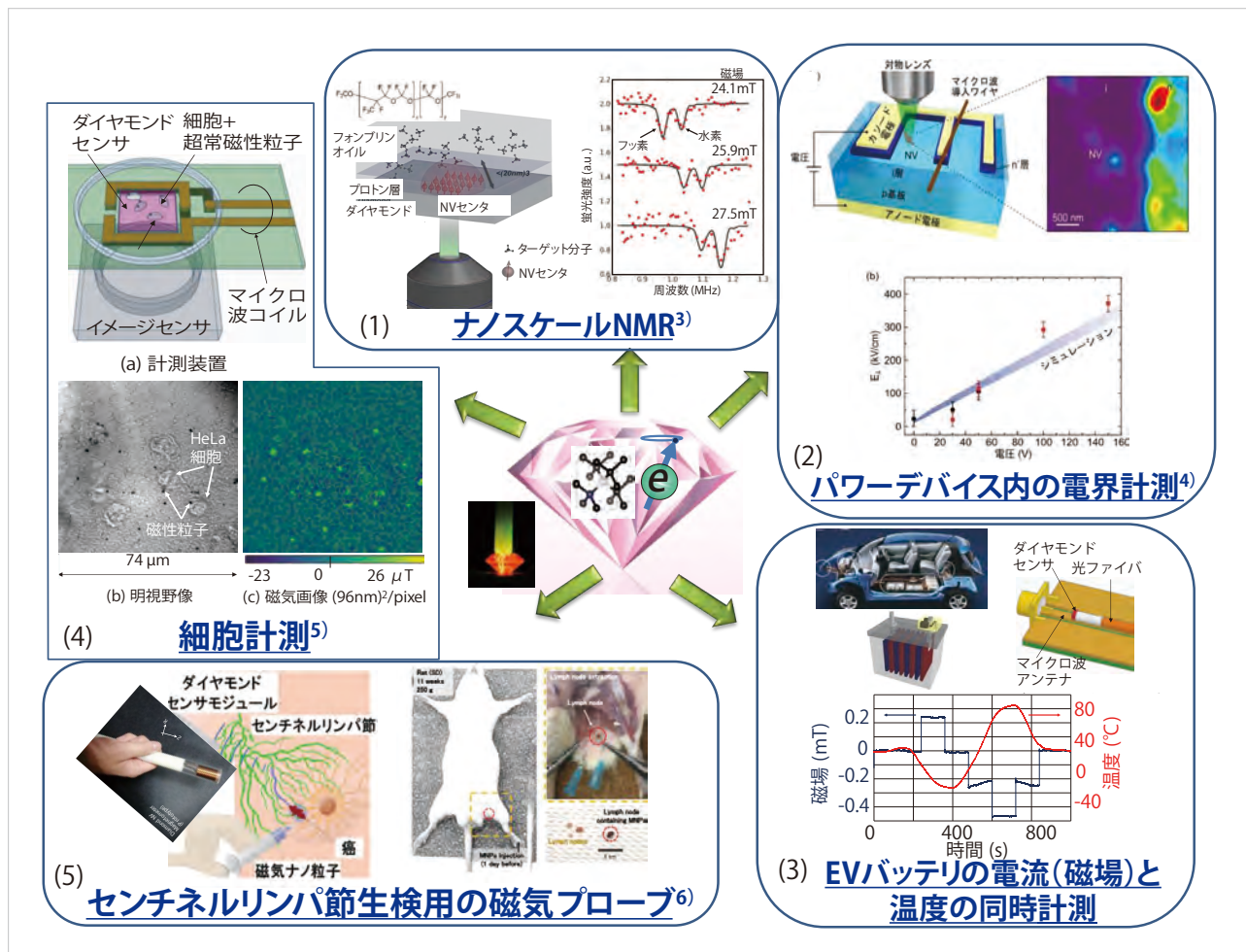
一方NVセンタは高感度である上に、ダイヤモンドセンサの表面に試料を密着させられることから、ナノスケールの体積中の 10^4 程度の核スピンを検出可能である。AC磁場の検出においては、ACの半周期ごとにNVセンタに共鳴するマイクロ波パルス照射してそのスピンの向きを反転し、AC磁場以外の雑音の影響を打ち消して高感度化する、ダイナミカルデカップリングという量子センサならではのスピンの操作が適用可能である。このため、ナノスケールNMRは、NVセンタの特徴を活かした計測

の1つである。

ダイヤの表面に約1nm程度の炭化水素層を介して、フッ素を高濃度に含むフォンブリンオイルの計測を行った結果を、図-5(1)に示す³⁾。検出された2つのピークは、磁場を変化させピークのシフトを測定することで、水素、フッ素の核スピンの信号であることが確認できる。また、このピーク高さからNVセンタの深さを算出するとおよそ9.2nmであり、検出体積を見積もると、約 5.2×10^{-21} Lと極微量であることが分かった。

(2) パワーデバイス内の電界計測

ナノスケールでのエネルギーデバイスのモニタリングとして、パワーデバイス内部の電場分布の計測



■図-5 ダイヤモンド量子センサの原理検証 (例)

を行っている⁴⁾。絶縁破壊がパワーデバイスの耐圧を決定するため、保持できる電場の強さを知ること、パワーデバイスにとって重要なパラメータである。しかしながら、従来のセンサではデバイス内部の電界を直接定量することは困難であった。デバイス内にNVセンタを内包することで逆バイアス下での電場を定量検出できており、他の手法では測定困難な状況でも計測できることを示している(図-5(2))。

(3) EV用のバッテリーの電流と温度の同時計測

電池の充放電電流を模擬した $+0.5\text{mT} \sim 1.2\text{mT}$ の印加磁場、および $-40^\circ\text{C} \sim 85^\circ\text{C}$ の温度変化をダイヤモンドセンサにより検出した。さらに、磁場と温度を分離かつ同時に計測することに成功している(図-5(3))。

(4) 細胞計測

図-5(4)に示すように磁性粒子によるHela細胞に付随するダイナミックな磁気イメージが得られ⁵⁾、神経ネットワークの計測等へ応用可能である。光障害がないため、長時間に渡る生きたままの細胞計測が可能となる。今後、バイオエンジニアリングや創薬などイノベーションへの展開が期待できる。

(5) 乳癌のセンチネルリンパ節生検用の磁気プローブ⁶⁾

癌の性状を特定するために、ダイヤモンド量子センサを用いて、癌組織近傍に投与され、リンパ節中に蓄積された磁性ナノ粒子を検出する。量子センサを用いることで、検出距離が伸長され、個人差によらずリンパ節を検出可能とする。外科医による術中使用も視野に入れ、磁気センサモジュールを試作してハンドヘルドプローブへと搭載した。動物実験を実施し、ダイヤモンド量子センサを用いて生体組織

内の磁気ナノ粒子を検出できることを実証している(図-5(5))。

ダイヤモンド量子センサの研究は、世界的に競争が激しく日々新しい結果が公開される状況である。国内外を含むレイヤ間の連携、および異分野間の融合の促進が重要である。量子技術の特長を活用することにより、今まで得られなかったデータを取得し、さらに本会に関連する研究者の方々とタグを組めば、新たな価値を社会に展開できるイノベーションにつながると信じている。

特に脳や神経などの生体計測技術の革新は、ヘルスケア、脳疾患の予防や治療などの医療、さらには脳型情報処理などの応用に繋がると考える。たとえば、脳情報からのマインドリーディングによる新たなサービスの提供、脳科学を活用した新しい探索エンジンの登場が予測されている。常温大気下での高感度化に加え、装置の小型化が実現すれば、特に超高齢化社会での大きな寄与が期待される。

参考文献

- 1) Neumann, P. et al. : Science 329, 542 (2010).
- 2) Le Sage, D. et al. : Nature 496, 486 (2013).
- 3) Ishiwata, H. et al. : Appl. Phys. Lett. 111, 043103-1 ~ 5 (2017).
- 4) Iwasaki, T. et al. : ACS Nano 11, 1238 (2017).
- 5) Hatano, Y. et al. : Physica Status Solidi (A), 215, 22-1800254 (2018).
- 6) Kuwahata, A. et al. : Scientific Reports 10, 2483 (2020).

(2021年1月1日受付)

謝辞 本研究は、文科省光・量子飛躍フラッグシッププログラム(Q-LEAP) JPMXS011807395により行われました。

■波多野睦子 hatano.m.ab@m.titech.ac.jp

東京工業大学工学院教授。慶應義塾大学卒業後、日立製作所中央研究所入社。途中フォルニア州立大学バークリ校客員研究員。2010年より現職。現在応用物理学会会長。

[面白い量子技術]

8 量子暗号の原理と実用化に向けた動向

—絶対安全な通信の実現に向けて—



水谷明博 | 三菱電機（株）情報技術総合研究所

現代暗号と量子暗号

現代において暗号は必須の技術である。たとえば、ブラウザで Web サイトにアクセスする場合、Web サイトの URL が https で始まっているとブラウザと Web サーバ間で暗号通信が行われている。これにより、機微なデータの盗聴、改ざんや通信相手のなりすましを防ぐことができる。この暗号通信では、RSA 暗号や楕円曲線暗号などの公開鍵暗号と AES や Camellia などの共通鍵暗号が使われている。このような普段我々が使っている暗号を現代暗号と呼ぶ。一方、量子暗号は現在実用化に向けて世界中で研究開発が進んでいる未来の技術である^{☆1}。

2つの暗号の相違点

はじめに、現代暗号と量子暗号の相違をまとめる(表-1も参照されたい)。まず、現代暗号は現代のコンピュータによる実装が可能である。暗号化の速度も高速であり、インターネットにさえ接続していれば通信距離の限界もない。一方、量子暗号は実装に専用の送受信機(たとえば、送信機にレーザー、受信機にアパランシェ・フォトダイオード)が必要になる。微弱な光を使って通信を行うが、その光は通信距離が延びるとより頻繁に損失が起こる。そのため、通信距離 100km で通信速度は 1Mbps 程度

である。機能に関して、現代暗号は鍵共有、秘匿、デジタル署名や関数型暗号など高機能な暗号を実現できる。量子暗号は鍵共有という機能を持つ。

安全性に関しては、現代暗号と量子暗号で質的に大きく異なる。たとえば RSA 暗号の安全性は、大きい桁の合成数の素因数分解が効率的に解けないという仮定のもとに成立している。共通鍵暗号も効率的な解読アルゴリズムが存在しないという仮定のもとに成立している。このように「解読には膨大な時間がかかるはず」という予想のもとでの安全性を計算量的安全性という。この安全性の暗号では、今後の計算機や解読方法の改良により安全性が損なわれる可能性がある。たとえば、素因数分解は、量子計算機があればショアのアルゴリズムを実行することで効率的に解くことができる。また共通鍵暗号も DES や MISTY は 20 年程度で脆弱性(鍵の全数探索より効率的な解読方法)が見つかっている。現在、公開鍵暗号は量子計算機でも解けない問題に基づく暗号方式の選定が米国標準技術研究所によって行われており、2024 年頃に米国標準方式が決まる予定である。しか

■表-1 現代暗号と量子暗号の比較のまとめ

	現代暗号	量子暗号
方式	RSA, AES など	BB84, 差動位相シフト方式など
実装	通常のコンピュータで実装可能	専用の送受信機が必要
速度	高速 (AES のハードウェア実装で数 Gbps)	低速 (1Mbps 程度)
距離	限界なし	数 100km が限界 ^{☆2}
機能	鍵共有, 署名, 秘匿など高機能	鍵共有
安全性	計算量的安全性	量子力学に基づく安全性

☆1 量子暗号というと、量子力学の性質を用いた暗号タスク全般を指し、量子鍵配送 (Quantum Key Distribution, QKD) はその一例である。ただ、最もよく知られ、実現に近い技術が量子鍵配送であるため、本記事では量子暗号と量子鍵配送を同一視する。量子鍵配送以外の量子暗号に興味があれば、文献 1) を参照されたい。

☆2 数 100km という限界は、直接 2 者間で光を送受信した場合である。鍵共有の中継を行うノードがあれば、この限界を超えることは可能。

し、これも予想に基づく安全性にすぎず、いつでも今がショアのアルゴリズム発表前夜と同じ状況かもしれないという不安は残ることになる。一方の量子暗号は、量子力学という物理法則を安全性の根拠にしている。そのため、量子力学が正しい限りは量子暗号の安全性は決して脅かされることはない。

量子暗号の概要

量子暗号の目的

量子暗号は、以下の性質を満たす鍵 (K_A , K_B) をアリス (A) とボブ (B) 間に共有することを目的とする。

性質 1: 2 者の鍵は同一のビット列である。

性質 2: 第三者 (盗聴者) が持つシステムと鍵に一切の相関がない。

性質 3: 鍵の値の確率分布は一様ランダムである。

1 つ目の性質は 2 者間でビット誤りのないビット列を共有していることを示し、2 つ目の性質は鍵の値が第三者に漏洩していないことを示し、3 つ目の性質は 2 者が得る鍵は完全にランダムな確率分布から得られることを示して

いる。2 者がこのような鍵 K を n ビット共有している場合、鍵は一度使ったら使い捨てる運用 (ワンタイムパッド) のもとで、平文 M (n ビット) と排他的論理和を取ったデータ $M \oplus K$ を暗号文として伝送することで、無限の計算能力を持つ盗聴者に対しても安全な通信が可能になる。このような安全性を情報理論的安全性と言う。

量子暗号の前提

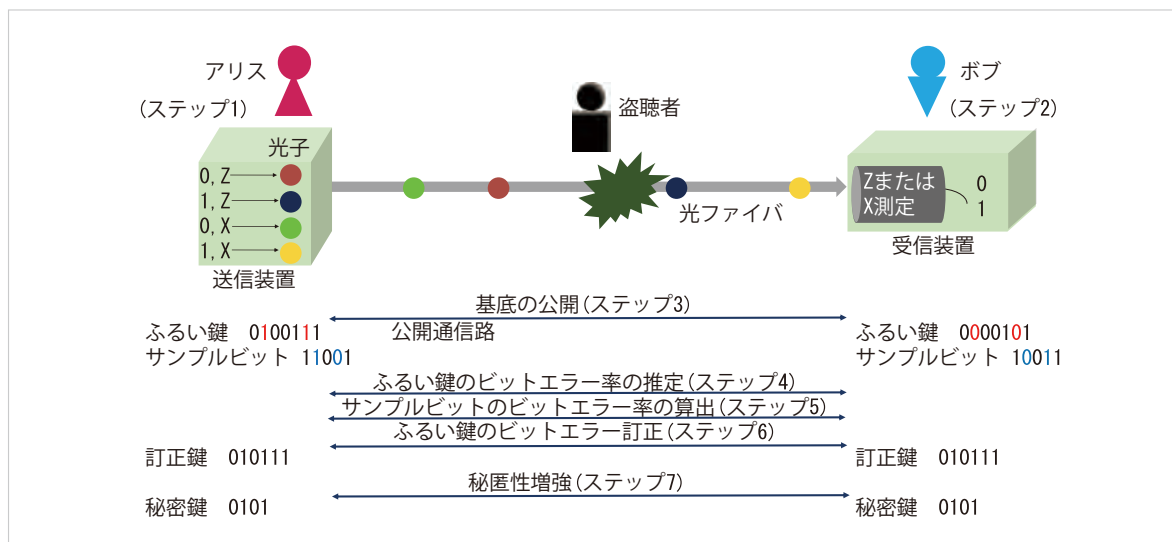
アリスとボブが持つ送受信装置の構成、通信路と盗聴者の前提をまとめる。図-1 も参照されたい。

送受信装置

アリスはランダムな乱数データを生成し、乱数データが載った光を送信する送信装置を持つ。ボブはアリスから送信された光の状態を読み取る受信装置を持つ。たとえば、送信機はレーザと偏光回転素子が、受信機はアバランシェ・フォトダイオードが使われる。

通信路

量子暗号では 2 種類の通信路が使われる。1 つが、乱数データが載った光を伝送するための量子通信路 (光ファイバ等) で、もう 1 つが認証された公開通信路 (電



■図-1 BB84 プロトコルの処理の流れ: (ステップ1) アリスはビット値と基底をランダムに選択し、対応する光子をボブに送る。(ステップ2) ボブは、Z または X 基底を選択し、その基底で光子を測定する。光子の送受信が終わった後、公開通信路を用いたデータ処理を行う。まず、(ステップ3) アリスとボブは選択した基底を公開し、ふるい鍵とサンプルビットを得る。その後、(ステップ4) ふるい鍵のビット誤り率を推定、(ステップ5) サンプルビットのビット誤り率を算出し、(ステップ6) ふるい鍵のビット誤りを訂正する。訂正鍵の一部の情報は盗聴者に漏れている可能性があるため、(ステップ7) 秘密鍵を得るために秘密鍵を得る。

話やインターネット等)である。盗聴者は、量子通信路を流れる光を好きに操作できるが、公開通信路を流れる情報は盗聴できるが改ざんできないと仮定する。

盗聴者

盗聴者は量子通信路を流れる光に対して量子力学で許されるあらゆる操作ができると仮定する。これは、物理の世界で許されるどんな操作でも行える最強の盗聴者を考えるという意味である。この「あらゆる操作」は、数学的にはトレース保存完全正写像として定式化される。詳しくは文献2)を参照されたい。量子暗号では通常、盗聴者がアクセスできるのは量子通信路と公開通信路のみで、アリスとボブが持つ送受信装置が置かれた部屋は完全にシールドされているとする。

代表的な量子暗号プロトコル

次に、上記で述べた性質1～3を満たす鍵の配送方法を、1984年にBennettとBrassardによって提案されたBB84を例に説明する。

送受信装置

送信装置は4つの光子^{*3}の偏光状態 $\{|0_z\rangle, |1_z\rangle, |0_x\rangle, |1_x\rangle\}$ のいずれかを放出するものとする。ここで $|0_z\rangle, |1_z\rangle, |0_x\rangle, |1_x\rangle$ は、それぞれ0, 90, 45, 135度の方向に振動する光子の偏光状態を表す。 $|0_z\rangle=(1, 0)^T$ と $|1_z\rangle=(0, 1)^T$ を2次元ベクトル空間の正規直交基底に取り、Z基底の状態と呼ぶことにする。すると $|0_x\rangle, |1_x\rangle$ は各々2次元ベクトル $|0_x\rangle=(|0_z\rangle+|1_z\rangle)/\sqrt{2}$ 、 $|1_x\rangle=(|0_z\rangle-|1_z\rangle)/\sqrt{2}$ と表現でき、これらをX基底の状態と呼ぶ。アリスはランダムにビット値 $a \in \{0, 1\}$ と基底 $b \in \{Z, X\}$ を選択し、 $|a_b\rangle$ をボブに送る。ボブは測定基底を $\{Z, X\}$ からランダムに選択し、受信装置を用いてその基底で測定することで測定結果を得る。測定結果は{ビット0を観測, ビット1を観測, 光子を観測しない}のいずれかになる。光子を観測しない事象は、通信路での光子の損失や受信機の効率が1でないなどの理由により起こる。

BB84 プロトコル

BB84 プロトコルの流れは以下である。図-1も参照されたい。

1. アリスはビット値とZまたはX基底のいずれかをランダムに選択し、選択したビット値と基底に対応する光子の偏光状態を、量子通信路を通じてボブに送る。この操作をN回繰り返す。
2. ボブは、ZまたはX基底を選択し、選択した基底で光子を測定して測定結果を得る。この操作をN回繰り返す。
3. アリスとボブは、選択した基底を公開通信路で公開する。アリスとボブが共に同じ基底を選択したビットのうち、Z基底を選択したビット値をふるい鍵、X基底を選択したビット値をサンプルビットと呼び、基底が一致しないビット値はすべて破棄する。
4. アリスとボブはふるい鍵の一部を、公開通信路を通じて公開し、公開していないふるい鍵のビット誤り率を推定する。この推定結果を e とする。
5. アリスとボブはサンプルビットを公開通信路で公開し、サンプルビットのビット誤り率 e_x を算出する。
6. ふるい鍵のビット誤り率 e が誤り訂正可能な閾値よりも低い場合、アリスとボブは誤り訂正符号を用いてビット誤りを訂正する。訂正後にアリスとボブが共有する鍵を訂正鍵(R_A, R_B)と呼ぶ。
7. アリスとボブは訂正鍵に対して秘匿性増強を行うことで、秘密鍵(K_A, K_B)を共有する。

ここでステップ7の秘匿性増強は、大体秘密な乱数を完全に秘密な乱数にする統計処理である。実際の操作は、訂正鍵(R_A, R_B)に行列要素がランダムな値を持つ行列を作用させることに対応し、作用の結果が秘密鍵(K_A, K_B)になる。ステップ6のビット誤り訂正が鍵の性質1を満たすため、ステップ7の秘匿性増強が性質2と3を満たすために行うデータ処理である。なぜ、秘匿性増強を行った後の秘密鍵が第三者に一切漏洩しないかを次で説明する。

*3 光子は電磁波におけるそれ以上分割できないエネルギーの最小単位である。

量子暗号の安全性

不確定性原理

量子暗号の安全性は量子の持つ不思議な性質である不確定性原理を根拠にしている。不確定性原理は、量子状態の測定と密接に関連している。例として、 $|0_x\rangle$ を Z または X 測定することを考える。Z 測定の測定結果の候補は $\{|0_z\rangle, |1_z\rangle\}$ であり、X 測定の測定結果の候補は $\{|0_x\rangle, |1_x\rangle\}$ である。測定者が Z または X 測定を選ぶことは、測定結果の候補を決めることに対応する。X 測定を選択したとすると、測定される状態 $|0_x\rangle$ は、測定結果の候補 $\{|0_x\rangle, |1_x\rangle\}$ に入っていることが分かる。そのため、 $|0_x\rangle$ を X 測定すると必ず $|0_x\rangle$ が測定結果になる。これは日常世界の言葉で言うと、コインが表の状態 ($|0_x\rangle$ に対応) で渡され、それが表 ($|0_x\rangle$ に対応) か裏 ($|1_x\rangle$ に対応) かを見ることに対応する。

ここで重要なのは、コインの状態は測定の前後で変化しないということである。日常世界ではこれは当たり前のことだが、量子の世界ではこの常識が成り立たなくなる。つまり、測定の前後で測定される状態が変わる場合がある。それが、 $|0_x\rangle$ を Z 測定した場合である。 $|0_x\rangle$ を Z 測定する場合、測定結果の候補 $\{|0_z\rangle, |1_z\rangle\}$ に $|0_x\rangle$ は入っていない。このような場合、測定後の状態はもはや $|0_x\rangle$ ではなく別の状態に変化してしまう。さらにこの変化は確率的に起こり、確率 1/2 で測定結果 $|0_z\rangle$ 、確率 1/2 で測定結果 $|1_z\rangle$ を得ることになる。確率 1/2 は測定結果が完全にランダムになることを意味するが、これは測定の仕方を上手く工夫すると確定的な結果が得られるように

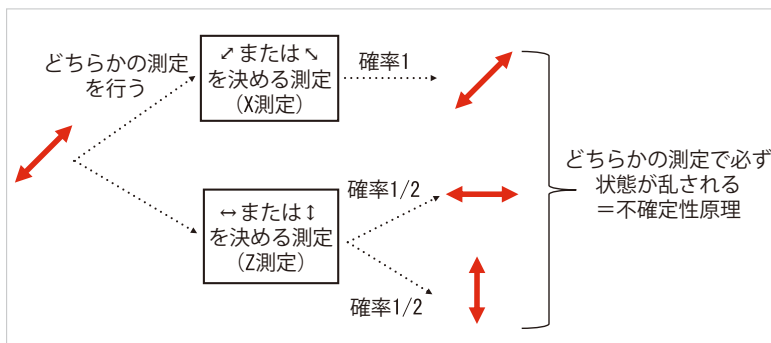
なるわけではない。どれだけ技術が進歩しても、この測定結果を予測することは不可能である。量子力学というゲームのルールから確率 1/2 になることが決まるのである。

まとめると、どんな量子状態も Z または X 測定すると、少なくとも一方の測定で必ず測定対象の状態が乱される。これを不確定性原理と呼ぶ (図-2 参照)。ここで説明した不確定原理は、情報エントロピーの言葉を使うと、 $H(W|Z)$ と $H(W|X)$ をそれぞれ Z 測定と X 測定をした場合の測定結果 $W \in \{0, 1\}$ の条件付きエントロピーとすると、 $H(W|Z) + H(W|X) \geq 1$ と表せる。エントロピーの和が 0 より大きいところに、測定結果の「予測のできなさ」という気持ちが現れている。

BB84 プロトコルの安全性

盗聴検知の仕組み

不確定性原理のおかげで、アリスとボブは量子通信路上の盗聴行為を検知することができる。例として、量子通信路を流れる各光子を Z または X 測定する盗聴者を考え、盗聴がどのようにして検知されるかを説明する。もし BB84 プロトコルのステップ 1 と 2 でアリスとボブが選択する基底が X で一致しているにもかかわらず、盗聴者が Z 測定すると、不確定性原理より光子の状態が乱される。その変化した状態をボブが X 測定すると、ボブが得る測定結果はアリスが選んだ乱数と異なるという事象が起きる。この事象が起きると、サンプルビットにビット誤りが生じる。つまり、盗聴者が間違っアリスとボブが選択した基底と違う基底で測定すると、その痕跡が「ビット誤り」という形でアリスとボブに検知されるのである。ここでは、Z、



■図-2 不確定性原理の説明：↔, ↑, ↓, ↙, ↘ はそれぞれ文中で定義した $|0_z\rangle, |1_z\rangle, |0_x\rangle, |1_x\rangle$ を表す。X 測定は測定結果が ↙ または ↘ のどちらか、Z 測定は測定結果が ↔ または ↑ のどちらかを決めることに対応する。↙ を X 測定すると状態は乱れずに ↙ がそのまま測定結果になるが、Z 測定をするとランダムな測定結果が得られ、状態は乱される。

特集

Special Feature

X 測定に限定したが、盗聴者がどれだけ複雑な攻撃をしても光子から情報を抜き取る操作を行うと光子の状態を乱してしまう。つまり、アリスとボブに気付かれずに情報を抜き取ることは原理的にできないのである。このため、ステップ 5 でアリスとボブが算出するビット誤り率 e_X が、どれだけ盗聴されていたかの度合いを表すことになる。ビット誤り率 e_X が大きければより多くの情報が盗聴されていることになる。ステップ 6 は、盗聴によって乱されたビット列を直し、アリスとボブで同一のビット列を共有するための手続きになる。

秘匿性増強で短くする鍵の量

ステップ 6 で得られる訂正鍵 (R_A, R_B) は、同一のビット列ではあるが、盗聴者に一部情報が漏れている可能性がある。そのため、ステップ 7 で盗聴者に情報が一切漏れていないことが保障される長さまで訂正鍵を短くする秘匿性増強を行う。上記の BB84 プロトコルに関して結果だけを述べると、2 値エントロピー関数を $h(p) = -p \log_2(p) - (1-p) \log_2(1-p)$ 、ふるい鍵の長さを M とすると、 M が無限の極限では $M \cdot h(e_X)$ だけ鍵を縮めるとステップ 7 で得られる秘密鍵は性質 1 ~ 3 を満たすことが示されている^{☆4}。どれだけ鍵を縮めると安全な鍵になるかを示すことを安全性証明という。この安全性証明では盗聴者の攻撃は一切制限しないため、例に挙げた Z, X 測定をする盗聴行為は一例にすぎない。たとえば光子を個別に操作せずに、量子通信路を流れる N 個すべての光子を同時に操作し、情報が最も抜き取れる最適な測定をすることも可能である。このような盗聴者に対しても、秘匿性増強で $M \cdot h(e_X)$ だけ鍵を縮めると、安全な鍵が得られるというわけである。しばしば量子暗号の説明で、「盗聴されたビット数分だけ鍵を短くすることで安全な鍵を得る」と言うが、量子力

学で許される最強の盗聴者が原理的に盗聴できる情報量の限界を「ビット誤り率」という古典的な情報を用いて推測できる点が、安全性証明の非自明さであり面白いところである。誌面の都合上この面白さを存分に説明できないが、安全性証明の詳細に興味がある方は文献 3) も参照されたい。

量子暗号の開発動向

ここでは、量子暗号の実用化に向けた世界の開発動向について述べる。表-2 も参照されたい。

中国

量子暗号の開発で世界をリードしているのが中国である。中国は 2017 年に衛星を用いた量子暗号の実証実験に世界で初めて成功している。具体的には、7,600km 離れた中国とウィーンの 2 点 (A, B) で鍵を共有するために、地点 A は鍵 K_A を、地点 B は K_B を量子暗号により衛星と共有する。その後、衛星が $K_A \oplus K_B$ を公開することで、 $K_A \oplus K_B$ を地点 A が自分の鍵に足して K_B を地点 A と B が共有するという仕組みである。衛星を信頼できる古典ノード^{☆5}として使うことで、大陸間での量子暗号に成功しているのである。また、2018 年には上海～北京におよぶ全長 2,000km の世界最大の量子暗号ネットワークを構築し、現在ではすでに ICBC などの銀行や保険会社がこのネットワークを利用している。今年の量子暗号

☆5 信頼できる古典ノードは、量子暗号では通信を行う 2 者以外は盗聴者と考えるが、中間の第三者も信頼できると仮定し、秘密鍵共有の中継を行うノード。

■表-2 量子暗号の実用化に向けた世界の開発状況のまとめ

地域	開発動向
中国	衛星を用いた大陸間での量子暗号通信に成功。世界最長の量子暗号ネットワークを構築し、実運用が開始している。
米国	Quantum Xchange 社が金融機関向けに、量子暗号通信サービスの運用開始を発表。
欧州	ユースケースが設定された 16 個の量子暗号拠点を欧州全域に作り、各拠点でのユースケースの実施と、拠点を相互接続するテストベッドプロジェクトが始動している。
日本	東京 QKD ネットワークの試験運用の継続と、医療データの秘密分散に QKD ネットワークを活用する独自の試みを実施。

☆4 量子暗号の安全性証明では、秘匿性増強で訂正鍵を短くするビット長を推定する際、確率論における集中不等式 (Hoeffding 不等式や Azuma の不等式など) を用いる。ふるい鍵の長さ (M) が有限の場合、推定量の期待値からのずれ (統計誤差) を考慮する必要があり、安全性証明が煩雑になる。そのため、多くの安全性証明では証明の簡単のため、ふるい鍵の長さは無限とすることで統計誤差を無視している。もちろん、ふるい鍵の長さが無限というのは現実的でないため、代表的な量子暗号プロトコル (BB84 や総当たり差動位相シフト方式など) では、ふるい鍵の長さが有限の場合の安全性証明 (有限長解析) も行われている。

特集 Special Feature

の国際会議 QCrypt 2020 で発表があったが、今後は小型衛星や小型地上局の開発を行い、地上のネットワークを中国全土に拡大する構想があるようである。

米国

米国では、2018年に量子通信の企業 Quantum Xchange 社が、ウォールストリートにある金融機関を顧客ターゲットにした米国初の量子暗号通信サービスの運用開始を発表した。現在は、ボストン～ワシントン DC 間の 800km のネットワークだが、今後はアメリカ中部、西海岸まで拡大する計画があるようである。

欧州

欧州では、2019年から大規模な量子暗号プロジェクト (Open QKD) が始動している。これは、約 1,500 万ユーロを投じ、2022年までに欧州全域に 16 個の量子暗号拠点を作り、それらを相互接続するテストベッドプロジェクトである。16 個の拠点は、ウィーン、プラチスラヴァ、オストラバ、グラーツ、ノドバ、マテラ、アテネ、バルセロナ、オーバープファッフェンホーフェン、ジュネーブ、ノリ、ケンブリッジ、デルフト、マドリッド、ベルリン、ポーゼンである。各拠点で量子暗号のユースケースが設定され、量子暗号リンクを設置する計画である。すでにジュネーブでは 6 個の量子暗号リンクの設置 (各リンク間の距離は 5 ~ 10km) が完了し、すでにユースケースが始まっている。今後は、オーストリア、スペイン、ドイツでの量子暗号リンクの設置が始まる予定である。

日本

日本は、2010年に東京 QKD ネットワークテストベッドを構築し、現在も試験運用を行っている。このネットワークは、都内に敷設された光ファイバを使い、4 拠点 (大手町、白山、本郷、小金井) を結ぶ総延長 200km ほどのネットワークである。また 2019 年には、NICT と NEC が量子暗号と秘密分散^{☆6}を組み合わせ、医療データや生体認

証データを管理するシステムを開発している。量子暗号ネットワークを 2 地点間の秘匿通信だけに利用するのではなく、データの分散バックアップに利用するという独自の活用も行っている。

今後の展望

量子暗号は現代暗号と比較して導入コストが高いと考えられる。ただ、世界の開発動向で述べたように、徐々に量子暗号の利用が広まっている状況を踏まえると、今後需要がさらに高まれば、量子暗号装置の価格も下がっていくことが予想される。量子暗号は鍵共有という用途に限定されるが、もし価格が数十万円となれば、量子暗号で (たとえば共通鍵暗号で使用) 鍵を配送しよう、という風潮が広まっても不思議ではない。このような将来が来るために、今後も量子暗号の理論家と実験家が協力して研究開発を進めることが不可欠である。現在、量子情報技術は世界中で活発に研究開発が行われているが、量子だからできる情報処理の実用化に最も近い技術が量子暗号である。究極のセキュリティという太古の昔から人類が求めてきた技術の実用化に向けて、我々も理論的な側面から研究開発を促進していきたい。

参考文献

- 1) Broadbent, A. and Schaffner, C. : Quantum Cryptography beyond Quantum Key Distribution, Designs, Codes and Cryptography 78, pp.351-382 (2016).
- 2) Nielsen, M. A. and Chuang, I. L. : Quantum Computation and Quantum Information, Cambridge Univ. Press., Cambridge (2000).
- 3) 小芦雅斗, 小柴健史 : 量子暗号理論の展開, SGC ライブラリ 67 (2008).

(2020年9月30日受付)

■水谷明博 Mizutani.Akihiro@dy.MitsubishiElectric.co.jp

2018年大阪大学基礎工学研究科物質創成専攻博士後期課程修了。博士 (理学)。同年三菱電機 (株) に入社。情報技術総合研究所情報セキュリティ技術部に所属し、量子情報の理論研究と情報セキュリティの開発を行っている。

^{☆6} 秘密分散は、データを無意味化されたデータに分割し、各々を異なる遠隔のサーバに保管することで、一部のサーバが棄損しても元データを復元できる技術。

[面白い量子技術]

9 量子コンピュータハッカソン —コミュニティによる量子人材育成—



小林有里



松尾惇士



沼田祈史

IBM Research - Tokyo

量子人材育成の必要性

量子コンピュータは、従来のコンピューティング手法とは根本的に異なる仕組みを使って計算を行う新しいコンピュータだ。IBMは2016年に世界で初めてクラウド型量子コンピュータを無償公開した。この量子デバイス上での量子計算を可能とするオープンソースの量子ソフトウェア開発キットであるQiskitは、現在までに、50万回以上ダウンロードされ、ユーザは28万人を超える。また、世界最大の30台の量子コンピュータを常時稼働させ、これまでに、数千億の量子回路を実行している。現在、研究開発段階にある量子コンピュータだが、今後、量子コンピュータの技術革新が進むと、その得意とする分野では従来型コンピュータを凌駕する性能を持つことが期待されている。たとえば、分子的または化学的相互作用プロセスの解明、困難な最適化問題への対処、人工知能の能力向上などが、近い将来の応用分野として挙げられる。

一方、量子コンピュータに関する専門教育は近年まだ始まったばかりであり、現在同分野で活躍する研究者や開発者の多くは、「物理、工学、情報科学等の専門教育をそれぞれに受けた人たちが、ある時点で量子コンピューティングにかかわることになり、互いの専門領域を学び合いながら」¹⁾ 技術の発展に取り組んでいる。

量子コンピューティングを専門的に学んできた人材は限られており、社会の実課題の解決に役立つ量子アルゴリズムの実装が可能となる(量子アドバンテージ)の時代がすぐそこまで来ていると試算²⁾される中、量子コンピューティングの未来を担う人材の育成と確保は重要な課題の1つとなっている。

学生や個人が量子コンピューティングを使用できるようになり、量子コンピューティング業界全体の技術力を高め、また将来を支える優秀な人材の育成のために何が必要とされているのか、具体的な取り組みを紹介する。

合宿型のハッカソン Qiskit Camp

ハッカソンとは、あるテーマに沿って、短期間集中型でプログラミングを行うイベントである。その場で開発される新しいアプリケーションやサービスによる実用的な利点だけでなく、参加者のスキル向上も期待できる。特に専門の教育が始まってまだ日の浅い量子コンピューティングの分野においては、この教育的側面が強く、また優秀な人材を発掘する場ともなる。

IBMは2019年に世界4都市で量子コンピューティングのための合宿型ハッカソンを行っている。参加者は短期間でQiskitを使った量子コンピューティングスキルを磨く機会が得られ、またさまざまなバックグラウンド

を持つメンバとチームを組み、第一線の研究者からコーチを受けながらプロジェクトに取り組むことができる。日本では Qiskit Camp Asia として、2019 年 11 月 18 日から 4 日間、主にアジア地域の 16 カ国から、約 150 人の学生、研究者を集めて山梨県で合宿を行った。上位入賞したチームのプロジェクトは量子コンピュータのデバイスを制御するプログラムの開発や量子機械学習、量子最適化のアプリケーション、また量子ゲームなど幅広い分野に及び、新機能の実装によるオープンソースコミュニティへの貢献につながっている。

オンラインの 量子プログラミングコンテスト

Quantum Challenge の概要

IBM Quantum Challenge はオンライン型の量子コンピュータをつかったプログラミングコンテストとして 2019 年 9 月に第 1 回が開催され、世界 30 カ国以上から 800 名近くが参加した。第 2 回目の IBM Quantum Challenge が 2020 年 5 月、IBM の量子コンピュータがクラウド上に公開されてから 4 周年を記念するイベントとして開催され、1,745 名が 45 カ国から参加し、イベント期間中の 4 日間で、量子計算が 1 日合計 10 億回以上実行される快挙を成し遂げた。2020 年 11 月には第 3 回目の IBM Quantum Challenge が開催され、限定 2,000 人枠をめぐり世界 85 カ国から 3,300 名以上が応募するまでに成長した。

初年度 (2019 年) の演習問題

オンライン型量子プログラミングコンテスト IBM

Quantum Challenge は、量子コンピューティングにまだ触れたことのない未経験者が、量子コンピュータの基礎から応用までを段階的に学習できるようにすることを目的としている。最初の数週間で実習を通じて量子プログラミングや量子アルゴリズムについて学んだあと、最終週では他の参加者と量子プログラムの効率を競い合う。表 -1 に 2019 年度の Quantum Challenge の週毎の演習問題課題を示した。

詳細は <https://github.com/quantum-challenge/2019> を参照のこと。次項では本戦の問題について解説する。

2019 年度の最終問題「コンビニ出店問題」

「IBM Quantum Challenge 2019」の最終問題は、前週までに学んだ知識やスキルを総動員して取り組む前提となっている。具体的な出題内容は以下のとおりである。

「東京の Z 市は 11 の区域からなる自治体で、すでに 4 社のコンビニ (A 社, B 社, C 社, D 社) が本社の 1 店舗を別々の区域に展開しています。

現在の出店状況は地図の通りです。地図上の各ノード (頂点) はそれぞれの区域を表しており、地図上のエッジ (線分) は、エッジの両端の区域が隣り合っていることを表しています。」(図 -1 参照)

これは「自治体のコンビニ出店プランを提示せよ」という問題で、複数のコンビニエンスストア・チェーンを市に誘致する際、各チェーン店舗 (色で示されている) から「同じチェーン店が隣接しないようにしてほしい」という条件を提示され、この条件に合致する出店計画の立案をせよという内容である。

グローバールのアルゴリズムと呼ばれる有名な量子アルゴリズムを用いて、問題の制約に基づく判定関数 (以下「オラクル」と呼ぶ) を構成することが問題を解く鍵となる。

この問題を数学的に考えると、「グラフの頂点彩色問題」として捉えることができる。グラフの頂点彩色とは、グラフの頂点に、ある制約条件を満たすように色を割り当てることであり、ここでは隣接するノードが同じ色

■表 -1 2019 年度 Quantum Challenge の演習課題

	演習課題
第 1 週	量子計算の基礎 (量子ゲート, 量子回路, 半加算器の構築)
第 2 週	量子アルゴリズムの学習 (グローバールのアルゴリズム)
第 3 週	量子アルゴリズムの応用 (グローバールのアルゴリズムを使った Max Cut 問題)
第 4 週 (本戦)	量子アルゴリズムをつかって複数のコンビニエンスストア・チェーンを市に誘致する出店計画を立案

特集 Special Feature

とならないよう色を割り当てるのが制約条件となる。

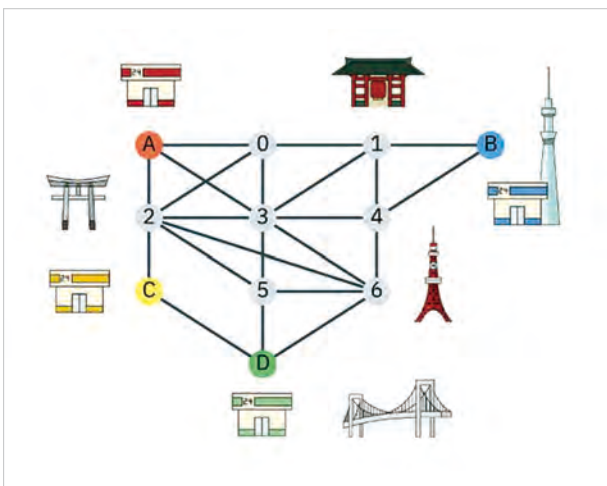
制約条件を判定するオラクルを作成するためには、隣接するノードが同じ色かどうか判定するために、まず各ノードに2量子ビットを割り当て、4色の色をそれぞれ00, 01, 10, 11のビット列で表現する。そして、隣接するノードのビット列が同じかどうかは、複数コントロールビットを持つ Controlled-NOT ゲートを用いることで可能である。すべてのエッジに対して両端のノードを比較し、その比較結果の AND を取ることで、与えられた色の割り当てが制約を満たすかどうか判定するオラクルを作成できる。

ただし使用可能な量子ビット数には32量子ビットと限りがあり、初歩的な解法の量子プログラムは実装することができないように設定されている。参加者は限られた量子ビットの中で効率の良い量子プログラムを実装するために工夫を凝らす必要がある。

2020 年度の演習問題

2020 年度の最終問題 — 惑星問題 —

2020年11月9日から30日まで開催された「IBM Quantum Challenge 2020」の最終問題は2019年度のさらなる応用版として、同じくグローバーのアルゴリズムをつかって解くことが前提となっている。出題内容は具体的には以下のとおりである(図-2参照)。



■ 図-1 IBM Quantum Challenge 2019 の最終課題の図

前提条件:

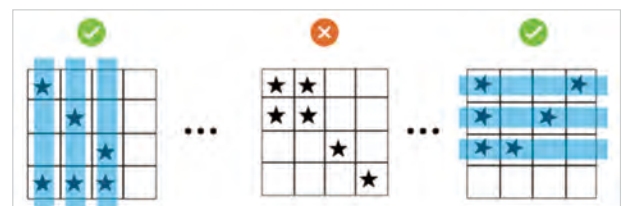
- 4×4の盤面が16個与えられている
- 各盤面に惑星が格子のマス内に置かれている
- 惑星の数は6である
- ビームを発射することで惑星を破壊できる
- ビームは垂直または水平方向にしか打てない
- ビームを発射できる本数は最大3本まで
- 16個の盤面中1つだけ上記条件では解けない盤面が混じっている

問題: 前提条件に基づいて解けない(惑星をクリアできない)盤面を特定せよ。

これは「惑星問題」と呼ばれる有名なパズルで、ここでは当然ながら、この問題を量子的に解くことが求められる。

Quantum Challengeではコンテスト期間中、各演習問題を解くためのヒントが提示されるが、最終問題においてもこのアプローチについてヒントとして提示を行っている。

この問題の解き方は多く存在するが、ここでは1つのアプローチを紹介する。それは、盤面に配置される惑星とビームの情報をそれぞれグラフのエッジとノードにエンコードし、惑星問題をグラフ理論における基本的な計算問題の1つである「頂点被覆問題」に変換して解く方法である(図-3参照)。頂点被覆問題とは、計算複雑性理論におけるNP完全に属する問題の1つで、与えられたグラフの各エッジについて端点のいずれか少なくとも一方が含まれるようなノード集合を求める問題である。盤面情報からグラフへのエンコードの際には、ビームの撃ち方をノードとし、ビームを結ぶエッジを両端のビームのどちらかで破壊できる惑星とする



■ 図-2 与えられた16個の盤面の中には、1つだけ条件に基づいて解けない盤面が隠されている。

特集 Special Feature

(たとえば、盤面上の3行4列目に惑星が存在する場合、3行目に撃つビームと4列目に撃つビームをそれぞれノードとし、それらのノード間にエッジを張る)。これにより、頂点被覆問題を解いた際の答えである要素数3以下のノード集合(本問題では発射できるビーム数が最大3本のため)が、すべての惑星を破壊するビームの撃ち方を表すことになる。エンコードしたグラフの頂点被覆問題を解くために、量子プログラム内で2つのオラクルを構築する。1つ目のオラクルでは、「選択したノードですべてのエッジがカバーされているかどうか?」の判定を行う。このオラクルはControlled-NOTゲートを用いたORゲートと加算器を使い、6つのエッジ(惑星)すべてがカバーされているか否かを判定することで実装可能である。2つ目のオラクルでは、「選択したノードの数(ビーム数)が3かどうか?」の判定を行う。こちらのオラクルでも加算器を用いて選択したノードの個数を判定することで実装可能である。選択したノードが両方のオラクルを満たす場合、その選択ノード(ビームの打ち方)で惑星問題を解くことが可能である。本問題では、16個の盤面の内から与えられた条件で解けない1つの盤面を見つける必要があるため、本アプローチでは2つのオラクルを組み合わせるさらに二重にグローバラーのアルゴリズムを実装する必要がある。

2019年と2020年どちらのIBM Quantum Challengeにおいても、上位チームの解法は審査員の予想をはるかに超えたものであり、各チームの創意工夫には驚かされた。上位チームの解法はGitHub上で

公開されている³⁾ので、興味がある方はぜひ一度、目を通してほしい。

スコアの算出について

現在IBMが技術開発を進めている量子システムは、ノイズのある小規模の量子システムである。そのため量子アルゴリズムの実装において、エラー率を高める要因になる2量子ビットのゲートや補助量子ビットの数を減らすことによって量子回路を効率化することが求められ、ここに競技性を見いだすことができる。IBM Quantum Challengeにおいても、参加者は正解にたどり着くプログラムの構築のみならず、そのプログラムの効率化をどこまで進められるかを競うことになる。スコアは回路の実装コストを測定することで決定され、以下の数式で算出された。

$$\text{コスト(スコア)} = S + 10C$$

上記算出式においてSは1量子ビットゲートの数、CはCNOT(CX)ゲートの数である。任意の量子回路は、1量子ビットゲートと2量子ビットゲートに分解することができ、2量子ビットゲートのCNOTの実装時のエラー率は一般的に1量子ビットゲートのそれと比較して10倍となる。そのため、回路の実装コストを評価するために、CNOTゲートを1量子ビットゲートの10倍に設定している。

量子人材育成の3つのドライバ

Open access, open source, education

IBMでは量子人材育成のための教育の推進には、大きく3つのドライバ(推進力)「Open Access」「Open Source」そして「Education」があると考えている(図-4参照)。

1つ目のOpen Accessは、2016年5月のIBM Quantum Experienceの発表に象徴される、量子システムの一般への開放にある。それまでは研究施設内の一部の人間しか扱えなかった量子コンピュータがクラウド上に公開されることによって、世界中の人が無償で

Hint 3
There are several ways to solve the final exercise. In this hint, I will explain an approach that is general and naive. The key idea is to convert an Asteroids problem into a so-called [Vertex Cover](#) problem.

How to encode an Asteroids problem into a graph

Asteroids problem

Each node represents a row/column.

- H_i represents i -th row.
- V_j represents j -th column.

Each edge represents an asteroid.

- Put an edge between node H_i and node V_j if there is an asteroid at (i, j) .

In the left example, choosing $\{V_1, V_2, V_3\}$ can cover all the edges. The solution exactly corresponds to shooting beams at column 1, 2, and 3 vertically in the Asteroids problem.

Then, create the following 2 oracles and combine into one.

- Oracle 1: Are all the edges covered by chosen nodes?
- Oracle 2: Is the number of chosen nodes 3?

Nodes that satisfy Oracle 1 and Oracle 2 represent the solution for the Asteroids problem.

Once you know how to implement the above, you can tell whether a given Asteroids problem is solvable or not. You're almost there! Good luck!

Dr. Ryoko

■ 図-3 コンテスト内で提示された最終問題のヒント

特集 Special Feature

実機の量子コンピュータ上での計算を試すことが可能となった。常時稼働する量子システムの数は当初3つだったが、その後増え続けており、またノイズの影響によるエラー率の改善なども継続的に行われてきている。2020年12月現在、30台の量子システムがアクセス可能となったことにより、今回の「Quantum Challenge」のような数千名規模の量子イベントの開催が可能となった。

無償で誰もが家に居ながら量子実験を試行できるプラットフォームの誕生は、量子コンピューティングに触れながら学習できる機会の大きな拡大につながったといえよう。

2つ目のドライバは量子計算に必要なソフトウェアのオープンソース化である。IBMでは2016年に自社開発した「Qiskit」と呼ばれる量子コンピュータでプログラミングを行うためのツールキットをOpen Sourceとして2017年に公開した。技術的にまだ黎明期にある量子コンピュータの分野で自社開発したソフトウェアをOpen Sourceとして公開することで、この分野における技術をコミュニティの力で高めていくことができる。コミュニティにより、QiskitはOpen Sourceとして公開後50万回以上ダウンロードされている。世界中のさまざまな技術者がQiskitを評価し、機能改善の提案やドキュメントの作成などの支援を行う非常に熱心な量子コンピュータファンによるコミュニティが形成されている。

このコミュニティこそが量子コンピュータの可能性を押し



■図-4 量子人材育成の3つのドライバ

し広げ量子コンピューティングの未来を担う人材を育成する土壌となっている。

量子人材の育成には、前述のOpen Accessによって量子システムが開放され、Open Source化されたQiskitなどのソフトウェアツールが拡充されるとともに、それらを目的に応じて使いこなすための知識とスキルを獲得して具体的な課題解決に活かしていくこと、そして3つ目のEducationが重要となる。たとえば、IBMは2019年にオンラインの量子コンピューティングの教科書「Qiskit Textbook」(qiskit.org/textbook)を公開した。Qiskit Textbookは現在世界110以上の教育機関で採用され、誰もがこのオープンソースの教科書にコミュニティを通じて貢献することが可能である。Qiskitをダウンロードしなくてもオンラインでコードを実行して結果を確認しながら読み進めることができ、理論と実践の両方からアプローチしたつくりとなっている。Qiskit Textbookはコミュニティの力によって内容の拡充をはかりながら、量子コンピューティングの専門教育の土台を築くために進化を続けている。

このほか、動画で量子プログラミングについて学べるYouTubeチャンネルのコンテンツをはじめ、世界のIBMの研究所で量子コンピューティングの第一線の研究者や技術者と一緒にインターンシップを体験できるプログラムや大学の一学期分に総統する講義内容を受講できるサマースクールの開催など、量子人材の育成の観点からさまざまな取り組みが行われている。こうした中、本稿で最終問題を紹介したQuantum Challengeのような量子コンピュータのハッカソンもまた、量子人材育成の観点から、さまざまな可能性を見いだすことができる。

教育的価値の可能性

前述のとおり、Quantum Challengeのようなオンラインハッカソンは、数週間にわたって、量子コンピュータのある応用例について、ある程度時間をかけてじっくり学習させるような設計をすることが可能である。そこに競技性やストーリー性を加えることで、いわゆるゲー

特集 Special Feature

ミフィケーションを活用した学習効果が期待される。先の Quantum Challenge においても週ごとに新たなストーリー展開が用意されており、参加者は物語の主人公として週ごとの演習課題に取り組むことになる。数々の有益なヒントを与えてくれるアドバイザーのような存在である Dr. リョウコが、実験の途中で量子世界に閉じ込められる事態となり、最終問題を解くことそのものが Dr. リョウコの救出劇にもつながる仕掛けとなっている。

図-5, 図-6 は 2020 年 11 月のハッカソン参加前後で、量子コンピューティングおよび Qiskit の理解とスキルレベルについて 10 段階のスケールで自己評価を申告してもらったアンケート結果である。参加者のアンケート集計からは、ハッカソン開始前の時点では多くの参加者が初心者レベルにあたる 1 または 2 に寄っていることが見える。これに対して、参加後の結果ではスキルの中央値が 5 または 6 に移動している。

この結果から、Quantum Challenge のような量子コンピュータハッカソンには、未経験者や初心者が短期間で効率良くこの新しい技術分野を学ぶ上で参加者自身が実感できる効果が示された。

こうした学習効果を得るための鍵としては、特定の量子アルゴリズムやその応用問題を段階的に学べるような問題づくり、ストーリーやゲーム性といった要素を盛り込むこと、そして参加者同士が違いに切磋琢磨しあいながら情報交換やサポートをしあえるオンラインコミュニティの存在が挙げられる。

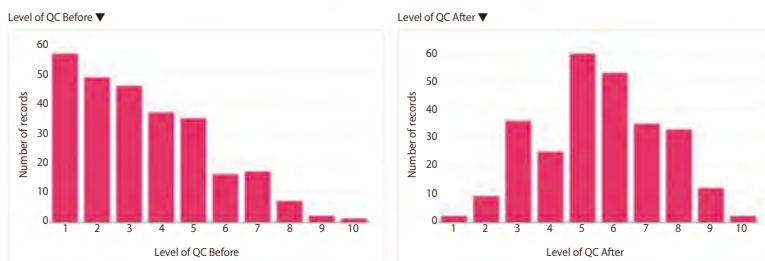
量子の未来のためのハッカソン

量子コンピューティングの未来を担う人材育成のために、今後も継続的な学習を支援するハッカソンやさまざまな学習体験を高める取り組みが期待される。しかし、どのような取り組みにおいても、人材育成には垣根を越えてつながることのできるコミュニティの存在がきわめて重要な役割を果たしていくことになるだろう。

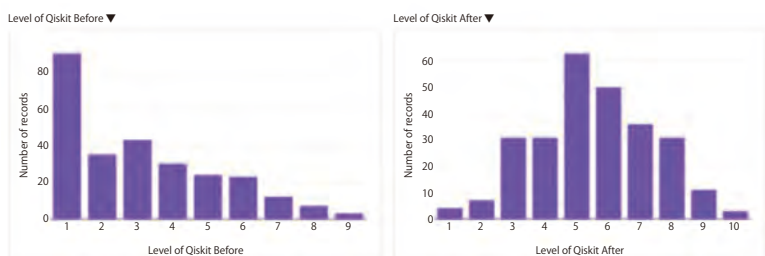
参考文献

- 1) MIT News : The Talent Shortage in Quantum Computing, <https://news.mit.edu/2019/mit-william-oliver-qanda-talent-shortage-quantum-computing-0123>
- 2) The Race to Quantum Advantage, <https://www.bvp.com/atlas/the-race-to-quantum-advantage/>
- 3) IBM Quantum Challenge 2020 (GitHub), <https://github.com/qiskit-community/IBMQQuantumChallenge2020>

(2021 年 1 月 19 日受付)



■ 図-5 量子コンピューティングに関する知識の変化



■ 図-6 Qiskit に関する知識とスキルレベルの変化

■ 小林有里 (正会員) yurik@jp.ibm.com

IBM の量子コンピュータ上で実行可能なプログラムを書くための Python ベースのオープンソース・ソフトウェア開発ツール「Qiskit」の開発者向けコミュニティを担当。量子コンピュータに関する研修やセミナー、大学での授業展開をはじめ、量子コンピュータを使ったプログラミングコンテスト、ハッカソンの主催などを通じて、量子人材の育成に注力。

■ 松尾惇士 (正会員) matsuo@jp.ibm.com

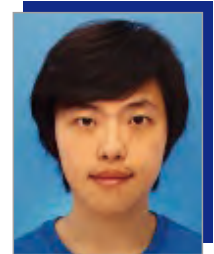
IBM で量子回路の最適化や量子コンピュータを用いた最適化問題用のアルゴリズムの研究を行っている。また Qiskit の開発にも注力している。第 1 回と第 3 回の IBM Quantum Challenge では問題作成と審査員も務める。

■ 沼田祈史 (正会員) kifumi@jp.ibm.com

IBM 入社後、ハードウェア製品の開発に従事。大学連携などの後、現在はカンタム・デベロッパー・コミュニティ所属。Qiskit Advocate としてセミナー、ハンズオン、プログラミングコンテストなどを開催。

[面白いぞ量子技術]

量子計算の未来を見据えて



長吉博成 | 東京大学

量子プログラミングコンテスト

近年、量子コンピュータに代表される量子情報処理への注目が高まるにつれ、さまざまな量子プログラミングコンテストが開催されるようになりました。これらのコンテストには、与えられた問題に正しく回答する競技プログラミングのような形式や、目的の計算をなるべく効率的に行うプログラムを作成するハッカソン形式などがあります。

私が今回参加した IBM Quantum Challenge は後者であり、3週間にわたって量子プログラミングについて初歩から学ぶことができるものでした。第1週では量子回路の基礎について解説されており、簡単なタスクをこなすことでその扱いに慣れていくための内容でしたが、第2週ではそれを応用してパズルの解法を求めるといふ、よりチャレンジングな問題が与えられました。さらに最終週のコンテスト課題では、制約の中であるべく低いコストの回路によって目的の計算を遂行することが求められ、将来の実用的な量子計算を見据えた実践的な内容となっており、とても刺激的でした。

こうしたコンテストは非常に教育的であるだけでなく、一見簡単な問題であってもそのアプローチは多種多様であり、背後に深遠で面白いテーマが隠れていることも少なくありません。現在多くの学生や社会人が競技プログラミングを通じてアルゴリズム設計や計算量理論を学んでいるように、ひよっとす

ると将来的には量子プログラミングコンテストが盛んに開催され、多くの参加者が鎬を削ることになるかもしれません。

量子計算—実験と理論

私は現在、東京大学工学部物理工学科の古澤・吉川研究室に所属しており、光を用いた量子計算に関する研究を行っています。量子コンピュータといえば、Google 社や IBM 社が近年精力的に研究を推し進めている超伝導方式が有名ですが、光を量子情報の担い手とする光方式ではエラーに頑健な量子ビットの実装が提案されている¹⁾ほか、現在の CPU のような原理的なクロック周波数の制限がないという利点があり、高速で省エネな量子計算の実用化が期待されています。

一方、光量子計算では、一部の量子操作の実装がきわめて困難であることが知られており、そのためリソース状態と呼ばれる特殊な状態を生成・利用して間接的に量子操作を施す手法が提案されています。私の卒業研究では、近年開発が進む超伝導測定デバイスを利用して「シュレディンガーの猫状態」と呼ばれる量子状態を生成する研究を行っており、光栄なことに本年度の優秀卒業論文賞および工学部長賞を受賞いたしました。

光を用いた実験に際しては、緻密な設計のもと定盤上に所狭しと配置された無数のミラーや光学素子

特集 Special Feature

を1つずつ手作業で精密に調整する、アライメントと呼ばれる作業を頻繁に行わなければなりません(図-1)。作業は大変ですが、チャンレンジを繰り返して最終的に目的が達成されたときの感慨もひとしおです。

このような実験面に加えて、私は現在、量子アルゴリズムの計算量理論に関する研究も行っています。たとえば、高速なデータ探索が可能になる Grover のアルゴリズム²⁾を用いることにより、巡回セールスマン問題やグラフ彩色問題などの計算量が古典計算機に比べて指数的に改善されることが分かっています。興味深いことに、量子アルゴリズムを一種のサブルーチンとして用いることで、



■図-1 光学定盤上でのアライメントの様子

その仔細に立ち入らずともさまざまな問題に対して古典より高速な量子アルゴリズムを設計することができます。特に、競技プログラミングで用いられるような見慣れた古典アルゴリズムであっても、その一部に量子性を導入することで思いもよらない計算量の改善が見つかり得るため、まるで宝探しのような面白さがあります。

量子計算はその誕生から日も浅く、今後どのような発展を迎えていくかはまったく未知数です。皆さんも、ぜひこうしたコンテストを通して、その面白さの一端に触れてみませんか？

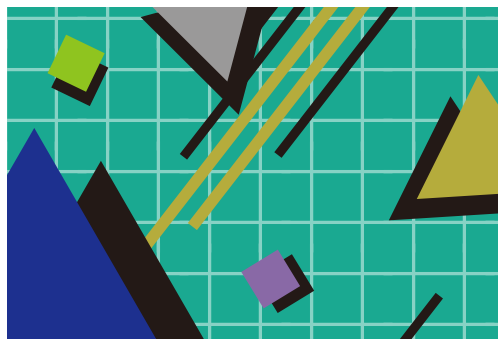
参考文献

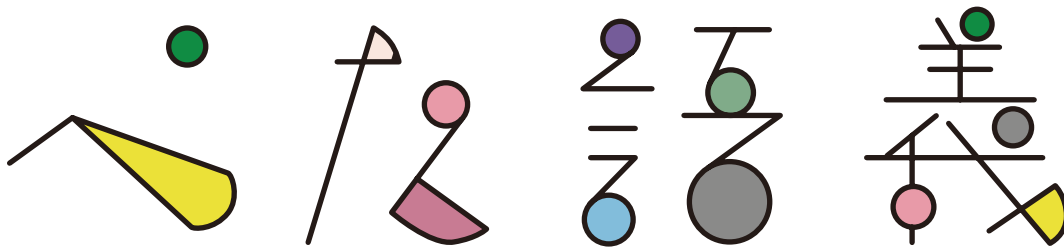
- 1) Gottesman, D., Kitaev, A. and Preskill, J. : Encoding A Qubit in An Oscillator, Physical Review A, 64(1), 012310 (2001), <https://doi.org/10.1103/PhysRevA.64.012310>
- 2) Grover, L. K. : A Fast Quantum Mechanical Algorithm for Database Search, Proceedings of The Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC'96, pp.212-219 (1996), <https://doi.org/10.1145/237814.237866>

(2021年2月25日受付)

■長吉博成 nano@g.ecc.u-tokyo.ac.jp

東京大学工学部物理工学科古澤・吉川研究室学士4年。現在、東京工業大学情報理工学院数理・計算科学系森研究室にてリサーチ・アシスタントとして勤務中。IBM Quantum Challenge Fall 2020 優勝。





Vol.115

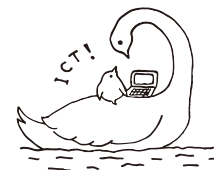
CONTENTS

【コラム】教育の ICT 化を推進するためには…前田 健太郎



COLUMN

教育の ICT 化を推進するためには



私が勤務する高校では、教育委員会から普通教室で情報の授業ができるのか試してほしいとの依頼を受け、84 台の Chromebook と G Suite を利用した実証実験を 2020 年 9 月から 2021 年 3 月まで行うことになりました。

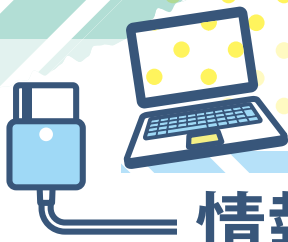
早速、校内の既設のネットワークに無線 LAN アクセスポイントを新たに設置し、Chromebook のネットワーク設定をしたのですが、道立高校のネットワークのセキュリティが原因で、Google アカウントを追加してログインすることができません。一方、コンピュータ室の PC からは Google アカウントでログインできますが、回線が混雑していて遅いという問題があります。コンピュータ室の PC で授業をしていたら実証実験の目的が果たせないのので、Chromebook を LTE 回線で接続して普通教室で授業をしました。情報の授業で利用する 42 台を手作業で充電しておき、休み時間に教室へ持って行かなければなりません。皮肉なことに、教育の ICT 化が業務多忙の原因になっています。

残り 42 台の Chromebook は他教科や総合学習での利用を目的に借りました。しかし、Chromebook は年度途中に導入されたので、ICT を活用した授業計画を立てている教員はいません。また、Chromebook を使ったことがない教員が多く、授業に Chromebook を使用することに抵抗感があるようでした。そこで、外部講師を招いて研修会を開いたところ、少しずつ授業で Chromebook が利用されるようになりました。すると、今度は授業で使いたいという教員が増えて、Chromebook の使い方やアプリについて質問されるようになり、利用希望が多くて貸し出しの調整が必要になったり、休み時間にパスワードを忘れた生徒がやってきましたと、ますます忙しくなりました。

2021 年 4 月からは GIGA スクール構想で設置された新しい校内のネットワークが稼働します。しかし、高校には一人一台の PC やタブレットはなく、BYOD (Bring Your Own Device) による個人所有の端末の利用が検討されています。ネットワーク環境があっても PC やタブレットがない状況では、新年度に ICT を活用した授業計画を立案することは困難です。生徒の個人所有の端末を授業で利用することにしたとしても、端末やネットワークの設定、トラブル等への対応が必要になるでしょう。これらの問題に対応できる人材が学校にいないければ、教育の ICT 化が進まないのではないのでしょうか。ネットワーク担当者がいない本校では、今年も情報科の教員が忙しい一年になりそうです。

前田健太郎 (北海道札幌北高等学校) (正会員) k_maeda@hokkaido-c.ed.jp
北海道札幌北高等学校、北海道高等学校教育研究会情報部会。

LOGOTYPE DESIGN...Megumi Nakata, ILLUSTRATION&PAGE LAYOUT DESIGN...Miyu Kuno



連載



情報の授業をしよう! =

本コーナー「情報の授業をしよう!」は、小学校や中学校で情報活用能力を育む内容を授業で教えている先生、高校で情報科を教えている先生や、大学初年次で情報科目を教えている先生が、「自分はこの内容はこういう風に教えている」というノウハウを紹介するものです。情報のさまざまな

内容について、他人にどうやって分かってもらうか、という工夫やアイディアは、読者の皆様にもきっと役立つことと思います。そして「自分も教え方の工夫を紹介したい」と思われた場合は、こちらにご連絡ください。

(E-mail : editj@ipsj.or.jp)



入試問題でテキストマイニング

中山享司 | 東京都立目黒高等学校

この授業の発端は、生徒募集のための、掲示物の検討からスタートした。本校では3学年に情報を設置している。そこで、生徒の進路意識を高めることもかねて、生徒に英語の入試問題を志望校ごとに分析させ、本校が手厚く進路指導をしていることをPRする材料にすることを計画した。実施にあたり、本校の英語科の先生を始め、さまざまな方からアドバイスをいただいた。今回その授業実践を報告する。

情報科とテキストマイニング

2013年度から行われている現行学習指導要領では、情報科の科目「社会と情報」「情報の科学」は選択必修修となっており、本校では「社会と情報」を設置している。「社会と情報」では、学習指導要領解説の、「(4) 望ましい情報社会の構築」の「ウ 情報社会における問題の解決」にテキストマイニングに関する記載がある。また、新学習指導要領解説においては、「情報I」の「(4) 情報通信ネットワークとデータの活用」におけるア(ウ)およびイ(ウ)にも記載がある。

授業実践について

先に述べた通り、本校では「社会と情報」を3年次に2単位(週2時間)行っている。受験勉強が本格化してくる2学期にテキストマイニングの授業を行った。以下に詳細を示す。

なお、本実践における手順および解説ビデオは、参考文献に記載した私の教材サイト(図-1)にてすべて公開している¹⁾。

実践1. 手作業で実施

第13回全国高等学校情報教育研究会全国大会(オ



■図-1 教材サイト

ンライン大会)での神奈川県立茅ヶ崎西浜高校の鎌田高德先生の発表内容を参考に授業計画を立てた。なお、私の授業実践の基となった鎌田先生の発表は、非常に分かりやすいので参考にさせていただければ幸いです²⁾。

授業のねらいは、後にパソコンを用いてテキストマイニングをするので、まずは感覚的に「テキストマイニングでこんなことが分かるんだ」という感覚をつかませることである。

授業の流れであるが、まずは手作業で歌詞をテキストマイニングさせた。手順は以下のとおりである。

教員が行う準備

1つのエクセルファイルに、

- 昔の曲3曲
- 最近の曲3曲

の歌詞を、シートを分けて打ち込む。

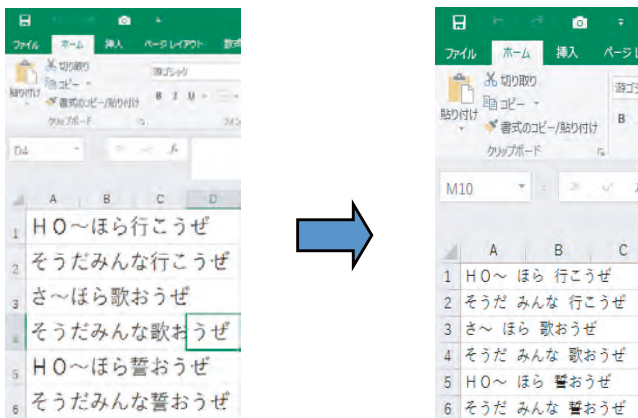
私はインターネットで歌を検索し、歌詞をエクセルに手入力した。

実践 (3コマ)

授業では、

1. 4人で1グループになる
2. 1グループにつき1曲担当させることにした。

歌詞は、2001年にリリースされたモーニング娘。の「ザ☆ピ〜ス！」(作詞・作曲：つくくみ)より引用。



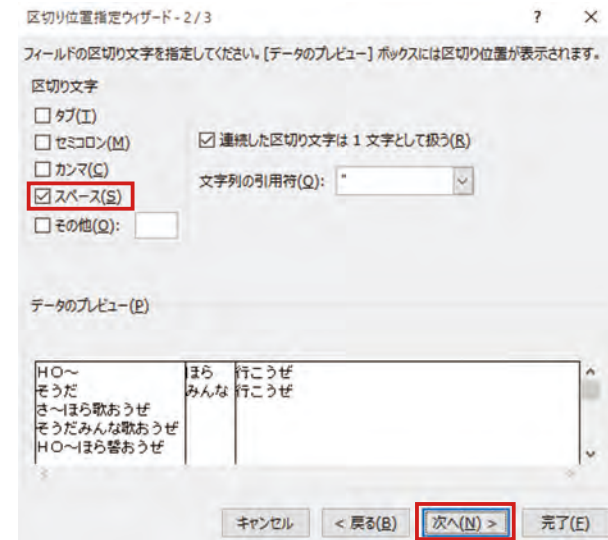
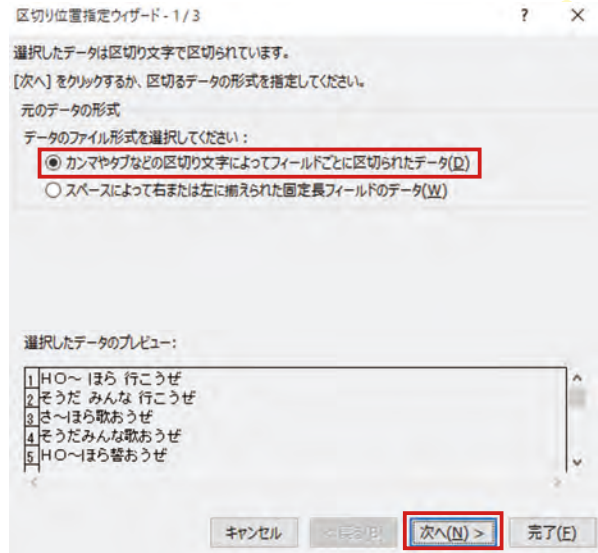
■ 図-2 打ち込んだ歌詞の一部

最初に、生徒に文節ごとにスペースを入れた。たとえば、「HO～ほら行こうぜ」という歌詞があったら、「HO～ ほら 行こうぜ」といった具合である。

文節で区切ったら、次はエクセルを操作し、1つのセルに1つの文節が入るようにする (図-2)。

具体的な操作は、エクセルの[データ]タブ→[区切り位置]を選択し、元のデータ形式は、[カンマやタブなどの区切り文字によってフィールドごとに区切られたデータ]を選択して[次へ]をクリックする。区切り文字は、スペースのみにチェックをする (図-3)。

[完了]をクリックすると、以下のように1つの



■ 図-3 区切り位置の画面

セルに1つの文節が入る。なお、分かりやすくするために罫線を引いて表示したが、罫線は自動では表示されない (図-4)。

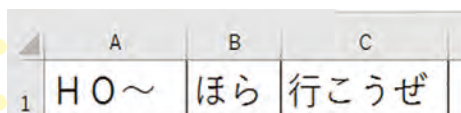
このように文節ごとに区切ったら印刷し、文節ごとに歌詞を切り分け、台紙に貼り付けていく。貼り付ける際には、品詞ごと(名詞・感嘆詞等)に分類したり、ポジティブ/ネガティブで分けたり、語尾に着目するよう指示をした。その結果、生徒たちは日本語と英語で分けたり、色を分けたりして作品を制作した (図-5)。

これは実際にやってみての反省であるが、紙を切り、貼り付ける作業がものすごく膨大になる。そのため、台紙に貼り付ける作業自体が目的となってしまう、本来やるべき傾向を探るといふ分析作業が疎かになってしまった。グループで1曲ではなく、1曲の半分にしてもよいと感じた。

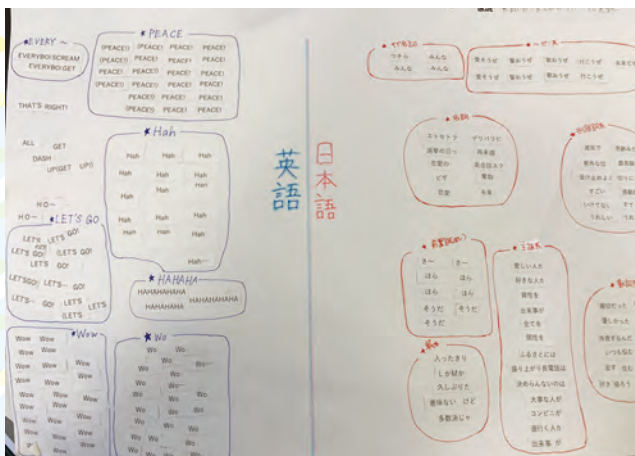
手作業での分析を終えたら、インターネット等で調べた情報も含めて、自分たちで分析した結果を発表させた (図-6)。

実践2. PCで実施

手作業でテキストマイニングを体験したら、今度



■図-4 区切られた文節



■図-5 手作業でのテキストマイニング

はコンピュータを使ってテキストマイニングを行う。使用するサイトは、ユーザーローカル社が提供しているテキストマイニングツールである (<https://textmining.userlocal.jp>)。

生徒が行う準備

指示は以下の通りである。

- テーマを定める(「バトルアニメの変化について」や「今と昔のスポーツアニメの曲」等)
- 昔の曲3曲, 最近の曲3曲の計6曲を分析する
- 昔と最近の曲の間は10年を目安に空ける
- 出力結果に対して考察する
- お手本(テンプレート)に沿って資料を作成する (図-7)

昔の曲・最近の曲ともに3曲分スライドを作成して提示した。

実践 (4コマ)

YouTubeのコメント欄に歌詞が載っているものについては、コピー&ペーストしてもよいという指導をした。しかし、歌詞がコピー&ペーストできないものについては手入力しなければならなかったため、分析することより入力することが目的になってしまっている生徒が散見された。

準備段階でお手本(テンプレート)を作成したので、生徒の作業に混乱は見られず、スムーズに授業が進んだように感じた。

最後の時間に相互評価を実施した。このときの相互評価はギャラリーウォーク形式にしたため、生徒

モーニング娘。	恋愛レボリューション2.1
目線	男女
雰囲気	ディスコのノリ
時代背景	21世紀の始まり
作詞者	つんく♂
歌詞の特徴	陽キャ 楽しい未来を予感させるような曲調
グループ	リーダーを務めていた中澤裕子のラストシングル

■図-6 生徒の発表資料



が特定の場所に密集することもあった。全員がまんべんなく評価がつくように追加の指示を出したが、相互評価のやり方に課題が残った（改善した手法は後述する）。

実践 3. 入試分析で実施

テキストマイニングでできることを体感した後、志望校の英語の問題に対してテキストマイニングを行い、入試問題の傾向をさぐらせた。

生徒が行う準備

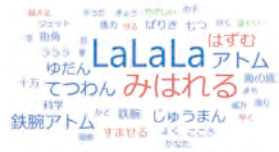
準備として生徒全員に以下のサービスのユーザ登録等をさせた。

- 某予備校の会員登録（入試問題をダウンロードするため）
- Google アカウントの作成（Google ドライブおよび Google ドキュメントを使用するため）
- ユーザーローカル社のテキストマイニングツールの会員登録（テキストマイニングが可能な文字数の上限を増やすため）

実践（素材の準備）

某予備校に会員登録すると過去問データベースにアクセスできるようになるので、志望校の英語の問題を5年分ダウンロードさせる。ダウンロードした

3 (昔) 鉄腕アトム

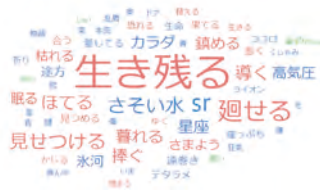


- LaLaLaやアトムに関する歌詞が多い
- 青色（ポジティブ）の名詞の表現が多い
- アトムの性能を歌っている

東京都立日暮高等学校 情報科

3

6 (今) マクロスF ライオン



- 生き残るという戦争中の渴望がでている
- 本気、君、見せつけるといった対話的な歌
- 歌詞のタイトルのライオンが何を指すのかよく分からなかった

東京都立日暮高等学校 情報科

6

1 例：ロボットアニメソングから見た時代背景

- 分析前の仮説
昔のアニメソングは必殺技やキャラクターの名前が入っていて、ロボットの宣伝を意識していた。最近の曲はロボットに関係のない曲が多いのではないかと

出席番号
氏名

東京都立日暮高等学校 情報科

1

2 分析した曲

- 1970～1980年代までのロボットアニメソング
 - 鉄腕アトム（鉄腕アトム,1980）
 - マジンガーZ（マジンガーZ,1972）
 - 機動戦士ガンダム（初代）（翔べガンダム,1979）
- 2000年代以降のロボットアニメソング
 - マクロスF（ライオン,2008）
 - 創聖のアクエリオン（創聖のアクエリオン,2005）
 - 機動戦士ガンダム00（Ash Like Snow,2008）

東京都立日暮高等学校 情報科

2

9 分析した結果

- 昔のロボットアニメソングは・・・
- 今のロボットアニメソングは・・・

東京都立日暮高等学校 情報科

9

10 一言で結論

- (昔) → (今)
- ロボットアニメは○○から△△に変化していると感じた

東京都立日暮高等学校 情報科

10

図-7 お手本として提示した資料

ファイルはPDF形式になっているため、そのままではテキストを選択することができない。そこで、ダウンロードしたPDFファイルをGoogleドライブにアップロードし、Googleドキュメントで開くようにする。すると、レイアウトは崩れるが、PDFファイルのテキストを選択することができるようになる。テキストを選択できるようになったら、英語の長文問題をコピーし、ユーザーローカル社のテキストマイニングツールに貼り付け、テキストマイニングを行う。テキストマイニングを実行した結果の、ワードクラウド(図-8左側参照)のPNG画像と、出現頻度をUTF-8形式でダウンロードする。ダウンロードが完了したら、出現頻度を見やすく整理する(図-9)。

最初はすべての品詞が縦一列に並んでいるため、それらを品詞ごとに並べ、条件付き書式のデータバーを用いて視覚的に頻度を表すようにする。整理

ができれば、PDF形式にエクスポートする。これを5年分用意して、素材の準備が完了する。なお、印刷の向きを横にしないと、名詞・動詞・形容詞の3つの品詞が入らないことがある。

実践(分析)

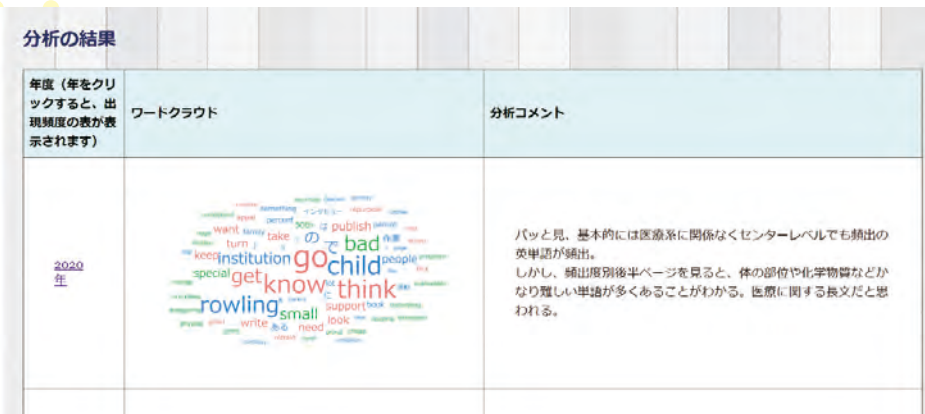
素材の準備が済んだら、分析方法について指導する。分析方法は本校の英語科教諭に相談した。その結果、以下のことを検討させるようにした。

【各年の分析として検討させたこと】

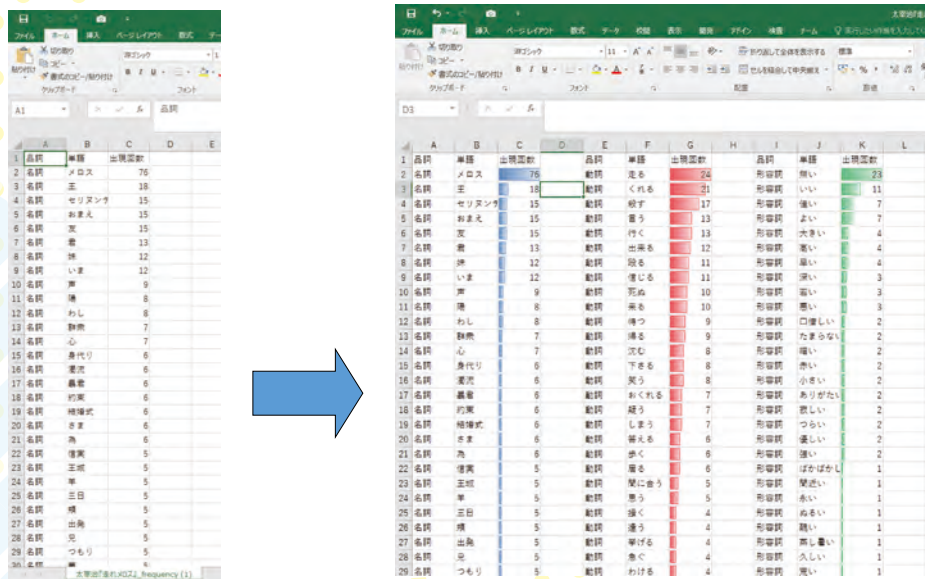
- 出現頻度の表を見て感じたこと(『簡単だと思った』だけから脱却できるとカッコいいですね』とあらかじめ指導した)
- 特に内容把握のために重要になる語は何か

【結論として検討させたこと】

- このような問題で入学させようとしている受験生



■図-8 Webページの例



■図-9 整理して表示した出現頻度



とは、どのような生徒か

- 何を学習するのが、得点をするために効率が良いか

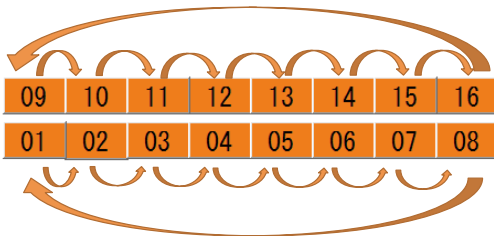
これらを検討させ、Web ページにまとめさせた(図-8)。なお、HTML、CSS の指導は歌詞分析と入試分析の間に、4時間かけてeラーニングで行った。

実践 (評価)

入試分析の結果を Web ページにまとめさせた後、相互評価を実施した。前回の反省を活かし、評価を付ける手順をあらかじめ定めた(図-10)。

評価の手順は次のとおりである

1. 作成した Web ページを自席の PC に表示する
2. 10 秒程度のインターバルをとり、隣の席に移動する



■図-10 相互評価の手順

3. 3分で評価を付ける(以後手順2,3を繰り返し)
これを繰り返すと、1番の生徒の作品に、2番～8番の生徒が評価を付けることになる。

私はこれまで、生徒一人ひとりを前に立たせて発表をさせるよう指導してきた。これには、全員の発表を見ることができたり、その場で個別に評価を伝えたり指導することができるというメリットがある。しかし、早く発表を終えた生徒と後の方に発表をする生徒とで公平性が保たれているのかという疑問も残る。さらに、40人学級の場合、一人3分の発表に加えて評価までさせようとする、全員が発表するまでに、およそ5～6時間使うことになり、授業時数を多く費やしてしまうといった課題がある。その点、相互評価の場合、上記のやり方だと20分強で評価を終えることができる。そのため、これまで5～6時間かけて行っていた評価の時間を削減し、余った時間を作業する時間に充てることができる。また、一人あたり7人しか評価が付かないという指摘もあるかと思うが、ループリックを用いて評価を付ければ、評価の平均値が大きく変わることもないだろうと考えられる(図-11)。

	S	A	B	C	D
デザインについて	Aに加えて、もともと用意していたひな形を一切使わずに独自に工夫しまとめられている	Webから用意した素材を随所に用いており、見やすいデザインになっている	テンプレートを用いて記述部を編集している	画像や分析コメントが乱雑に配置されており見づらい	不適切な表現がある
各年の分析について	Aに加えて、個人的な感想にとどまらず、さらに客観的に内容把握のための分析がなされている	出現頻度と問題文の両方を俯瞰した、本人なりの説明が随所にみられる	出現頻度または問題文のどちらかについての説明が記載されている	記載はされているが、何についての説明なのかが分からない	不適切な表現がある。または記載がない
結論の分析について	Aに加えて、各年の分析と結論とのつながりが明確にされており、「なぜこの結論になったのか」が一目瞭然であり、説得力のある内容である	分析結果をもとに、大学の意図を自分なりの意見で前向きに記載してある	自分の意見が書いてある	テンプレートの文言から変更されていない	不適切な表現がある。または記載がない

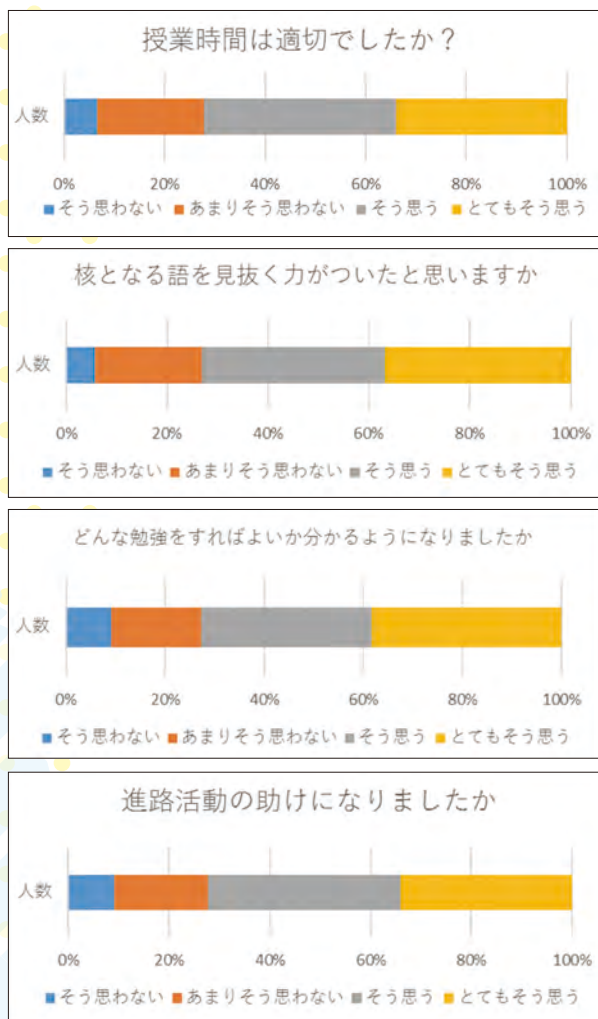
■図-11 実際に用いたループリック

振り返り

相互評価は20分強で終わるので、相互評価が終わったら、単元全体の振り返りのアンケートをとった(図-12)。

質問項目は下記5項目である。

- 授業時数は適切だったか
 - 問題の核となる語を見抜く力は付いたと思うか
 - 合格に向けてどんな勉強をすればよいか分かるようになったか
 - 進路活動の助けになったと思うか
 - 全体を通しての感想
- この結果を見て、次のように解釈した。
- おおむね7割の生徒から良い評価を受けた
 - おおむね3割の生徒が、何かしらの不満を持っている



■図-12 アンケート結果

ここで不満を持っていると回答した生徒の意見を以下に紹介する。

- 英単語だけを見てもよく分からない
- テキストマイニングをして、入試問題の何が分かるのか、最後までよく分からなかった。それならば、問題文を自力で翻訳したりしていた方が問題文の理解につながると感じた
- 問題は毎年異なる上に問題文に出てくる単語を分析したところで問題を解く手助けにはならないと思った

これらの意見を見て、テキストマイニングによって、単語の出現頻度や共起キーワードが分かるが、これをどのように分析すればよいのかという指導が不十分であったと感じた。この指導方法が今後の研究課題である。

今後の展望

冒頭に述べた通り、この授業実践のきっかけは、生徒募集のための掲示物を検討していたことである。しかし授業実践では、入試問題を分析することよりも、テキストマイニングの実施に重きを置いてしまったことが反省点である。生徒の反応を観察しながら授業を進めていくと、授業のねらい、目的の検討が不十分だったことに気づかされた。今回の実践を機に、テキストマイニングをはじめとするさまざまな分析手法について自ら学び、手法を手段として活用した授業実践ができるようにしていきたい。

参考文献

- 1) 中山享司：「情報科準備室」, <https://sites.google.com/view/takashi-nakayama/> (2020.11.7 閲覧)
- 2) キミのミライ発見 事例165 テキストマイニングによるアニソンの歌詞分析, <https://www.wakuwaku-catch.net/jirei20165/> (2020.12.12 閲覧)

(2020年12月20日受付)



中山享司 (正会員)
Takashi_Nakayama@education.metro.tokyo.jp

東京電機大学卒業。2011年情報科教諭として東京都に採用。2018年より東京都立目黒高等学校。



連載

★ Jr.

先生、質問です!



作り手によってAIの優秀さはどれくらい変わるのでしょうか？
 やはり、数学や、統計的なデータ分析を得意とする人が作ると精度は高くなるのでしょうか？
 はたまた、偏差値の低い人間が作ると精度は低くなるものなのでしょうか。
 ここでいう作り手は、自動的に完結するものではなく、自分で色々設定をずらしておきます。

匿名希望

【学生会員】大学生

AQ

現在のAIは、作り手によってその優秀さが大きく変わります。そのため、世界中のさまざまな企業がAI技術者の獲得競争を繰り広げています。また、開発したAIプログラムの性能を競い合う国際コンペも頻繁に開催されています。

優秀なAIを開発するためには、数学や統計的なデータ分析などの一般的な能力に加えて、AIを活用する分野特有の知見が非常に重要です。また、深層学習に代表される最近のAIには多数のパラメータが含まれていますので、その調整も非常に重要です。高性能な計算機を使って徹底的にパラメータ調整を行うことによって、AIの性能が飛躍的に向上することもあります。

これからAIを勉強する人は、データ解析の基礎となる統計学などの数学の理解と、AI実装のために必要なプログラミングの能力に加えて、画像、音声、ロボット、医学、化学、物理、金融など、AIを活用する分野に関する知識を身につけることが重要です。そして、未来のAIを開発する研究者を目指す人は、新しい数学の原理や、脳科学や認知科学などヒトの学習に関する知見、さらには、倫理や法制度などAIが実装される人間社会の理解など、多様な観点から今の常識にとらわれない自由な発想力を持つことが望まれます。



杉山 将
 【正会員】
 理化学研究所/
 東京大学

A



大岩秀和
 Google

AIの「優秀さ」とは何でしょうか。クイズであれば、なんでも記憶していること？ いち早く質問に答えられること？あるいは、早押しが上手なことでしょうか。「優秀さ」の定義方法はさまざまで、あらゆる面で優秀なAIは自分が知る限り存在しません。良いAIを作るためには、解決したい問題に合わせた「優秀さ」を上手く定義することが重要です。

数学や統計学は、「優秀さ」をより正確に測り、AIの中身をより深く理解するための重要な道具です。一方で、AIの研究開発・運用には、「優秀さ」の定義・AIを開発するための環境の整備・実際の運用など多様なプロセスで構成されており、コンピュータ科学などの他の知識も重要になります。複数人でAIを開発することも多く、全員が同じ分野に長けていることが重要とも限りません。

AIの良い作り手になるためには、数学や統計学に限らず、自分の持つ知識や経験をAI開発に活かす方法を考え実行できることが重要だと考えています。

「先生、質問です!」への質問はこちら



<https://www.ipsj.or.jp/magazine/sensei-q.html>



連載

ビブリオ・トーク
-私のオススメ-

小林真世 (愛媛大学 大学理工学研究科 兼 南予水産研究センター)

日本語から記号論理へ

齋藤正彦 著

日本評論社 (2010), 1,900 円+税, 184p., ISBN : 978-4-535-78554-0

日本語から記号論理へ



齋藤 正彦

あ!
記号論理だ。

日本評論社

「論理」から、皆さんは何を想像するでしょうか？
本会の会員の皆さんなら、「論理回路」や「ブール代数」、
「真理値表」といったものが多いのではないかと思います。
なかには、宇宙大作戦（あえて、Star Trek とは言いません）
でレナード・ニモイ (Leonard Nimoy) 演ずる Mr. スポックの台詞
「非論理的です」を思い出す年配者 (?) の方もおられるのでは
ないでしょうか。

私を含め日本語を母国語としている人は、物事を考えるのに、
日本語で考えています。皆さんも、何かの書物や文献を読んで、
その内容を理解しようとするときに、頭の中に、図を描いたり、
表を書いたりすることもあるでしょうが、言葉を使って、色々
と表現し、思考していると思います。もちろん、外国語が得意な
方であれば、その言葉で書かれた文献を読むときや、学会での
ディスカッションでは、外国語で考える場面もあると思いますが、
やはり、母国語である日本語を思考のための道具として使っ
ておられると思います。

さて、日本語と英語を比較すると、英語は「論理的」な言語
であるが、日本語は「非論理的」な言語で、論理的な思考をする
点では劣った言語であるといった話も聞きます。しかし、私は、
日本語が論理的な思考には適さない言語だとは思いません。英
語は、中学校、高校で 5 文型を習うように、例外はありますが、
文法によって主語や動詞、目的語などの順序が決まってお
り、単語は文のどこに位置するかで、役割が決まります。しか
がって、英語を話すときには、強く意識しなくても、主語を落
したり、目的語を落したりすることがありません。一方で、日
本語は、係助詞や格助詞によって、単語の役割が決まります。
文中でそれぞれの役割を果たす言葉は、比較的自由に位置す
ることができます。そのことから、日本語では、後で言うつも
りだった、あるいは、書くつもりだった言葉が、文の中で現
れないまま終わってしまうことがあります。このことが、曖

昧さをもたらししてしまいます。

このように、曖昧な表現を許してしまう日本語ですが、決
して「論理的」な議論ができない言語ではありません。誤り
なく表現する、伝えることを意識すればよいのです。そうす
れば、日本語でも、誤解のない表現が行え、論理的な議論
を行えます。

残念ですが、すべての日本人が「日本語は論理的な議論
に使える言語である」ということを知っているわけではない
と言えます。

前置きの話しが長くなりましたが、やっと、私が取り上げ
たい本の話にたどり着く準備ができました。

論文を執筆する、技術資料を作成する、報告書を執筆す
る、プレゼンテーションを行う、いずれの場合にも、読者や
聴衆に対して、自身の考えていることを、間違いなく伝える
必要があります。そのためには、曖昧さも許す日本語で、
曖昧性のない表現をする必要があります。「日本語から記号
論理へ」は、「眠れる森の美女」で「眠っている」のは「森」
なのか、それとも「美女」なのかといった話題から、「美
しい水車小屋の娘」や「病気で寝ている先生の奥さん」
といった典型的な曖昧表現を示しながら、読む人、聞く人
に誤解なく伝える方法・工夫について述べてところか始ま
っています。この導入部分で、私自身も、子供のときに聞
いた曖昧表現の例を思い出しながら「そうだったよな」と
か、「昨日のニュースの文も、曖昧で、あやうく間違っ
た理解をするところだったよ」とか思い巡らされること
になりました。分かりやすい例示から入っていくことで、
日本語の曖昧表現とその解消に結びつく表現に対する関
心をかき立てられます。さらに読み進めると、典型的な
曖昧表現のいくつかのパターンを示されることになりま
す。このあたりまでは、国語、いえいえ、「言語能力」と
言われる領域の書籍を読んでいるような感覚を覚えます。

その後は、日本語での表現で使われる「すべての(の)」や、

「任意(の)」といった全称量化詞, また, 「ある」や, 「少なくともひとつ」などの存在量化詞を含む表現, さらに, 量化詞を含む否定文に話題を移しながら, 量化詞を含む否定文の曖昧さの解説に踏み込んでいきます。

このあたりまで進むと, そろそろ記号論理の臭いがクンクンとしてきます。でも, 「言語」解説の範疇を踏み出し, 記号論理の世界に入る, その前に, 「命題文」と「論理文」の紹介, 解説があります。「命題文」は記号論理における「命題」に対応し, その真偽が定まった文です。「論理文」は, 記号論理における「論理式」に対応するものとして, 著者が独自に定義したものです。その詳細は……長くなりそうなので, 気になる人は, 書籍を手にとってご確認ください。

ここまで来ると, 記号論理の話題へと遷っていきます。ブール代数の講義だと, 一般的には, 「否定」, 「論理和」, 「論理積」といったところから入っていくのが一般的ですが, 著者が数学者ということもあるのでしょう, 記号論理の冒頭で「否定」を取り上げた後には, 「論理和」, 「論理積」と進まず, これらを後回しにして, 先に「全称量化」, 「存在量化」へと展開されていきます。皆さんの多くが, 大学入学直後, 量化記号「 \forall 」や「 \exists 」に, はじめて接したときに悩まされた人もいないでしょうか。この書籍が, 日本語を切り口として記号論理へと導くという流れをとった効果が発揮される点の1つは, 量化, 特に「二重量化」や「量子と否定」を, 日本語の曖昧表現とその解消と結び付けて解説している点にあります。書籍の冒頭部分で, 日本語の曖昧表現を通して, 曖昧さと正確さについて頭の中が整理されることによって, 量子に接したときに感じる難しさは, 大いに緩和され, すんなりと頭に入ってきます。また, 逆に, 量化から, 日本語表現を吟味し, 表現の曖昧さ, さらに, 誤解を生まない表現の考察へとつなげることもできるようになります。「日本語から記号論理へ」の逆「記号論理から日本語へ」の反映に結びついてきます。

書籍の中では, 先に触れたように, 量化についての解説のあとで, やっと論理積「 \wedge 」, 論理和「 \vee 」, 含意「 \rightarrow 」が取り上げられています。これらの説明も, 日本語の表現を示しながら解説しており, 大変分かりやすく書かれています。

書籍は, あと3分の1ほどが残っています。この残りの部分では, 記号論理の適用例として数学を取り上げています。著書自身は「記号論理がフルにその効力を発揮するのは, やはり数学と情報科学です」と述べています。私としては, 著者には, 数学ではなく, 情報科学分野を適用例として取り上げてほしいのですが, 著者は数学者ですから, そこは諦めることにしましょう。

さて, 私が『日本語から記号論理へ』を取り上げた理由は, 1つに記号論理への誘いとしての良書であると感じたこともあります。何よりも, 日本語による表現の曖昧さを, 記号論理を通して見直す眼力を養えるという点にあります。恐らく, 著者は, 日々用いている日本語とその表現から, 記号論理へと誘おうとしたのだと思いますが, 記号論理自身と記号論理と日本語表現との関係の理解が, 日本語表現の曖昧さを吟味し, 曖昧ではない表現を考える礎を与えてくれると思います。

シャノン (Claude Elwood Shannon) は, ウィーバー (Warren Weaver) との共著となる『通信の数学的理論』(筑摩書房, 原書名: The Mathematical Theory of Communication) の中で, 通信を3つのレベルに分けています。「レベルA: 通信において, 記号をどのくらい正確に伝えることができるのか。(技術的な問題)」, 「レベルB: 送信された記号は, どのくらい正確に所望の意図を伝えることができるのか。(意味的な問題)」, 「レベルC: 受信された意図は, どのくらい効果的に所望する行為に影響するのか。(効果の問題)」の3つです。誤解を生じない, 曖昧性のない文章を書くということは, レベルBの実現です。そして, この記事を読まれた皆さん, 特に, 学生や若い技術者・研究者の方々の「誤解のない日本語を書こうとする意識」を高めることができれば, 私自身にとっての「レベルCのコミュニケーション」が行えたこととなります。

さて, 最後にクイズを1つ, 「この原稿の中に, 曖昧な表現があります。それを見つけ出して, 曖昧性を含まない文に書き改めてください」。(2020年12月9日受付)

小林真也 (正会員)
kob@ehime-u.ac.jp

1985年大阪大学工学部通信工学科卒業。1991年大阪大学大学院工学研究科通信工学専攻修了。工学博士。金沢大学助手, 講師, 助教授, 愛媛大学助教授を経て, 2004年愛媛大学教授。





Listen, Attend and Spell :

A Neural Network for Large Vocabulary Conversational Speech Recognition

ICASSP (2016)

音声認識の方式を一新？

音声認識は、入力された音声をテキストに自動変換する技術であり、機械が音声言語を理解するために必須の技術である。音声は、同じ言葉（テキスト）でも、発話する人によって、そして環境などによってまったく異なるものになり、簡単な人手によるルールでこの自動変換をモデル化することは非常に難しいと感じていただけだろう。そこで、機械学習を駆使すべきタスクとして、これまでさまざまな音声認識の方式が検討されてきており、2020年現在で実用化されている主流の方式は、想像以上に長年のノウハウが詰まったものになっている。すなわち、音声認識という技術は、機械学習を用いれば簡単に実現できるというものではなかったというのがこれまでである。さて、本稿で紹介する論文は、長年のノウハウが詰まった音声認識方式を最新の機械学習の力で一新してしまうという流れの先駆けとなった論文である。以下では、「ノウハウが詰まったHybrid方式」と、この論文が提案する「独立仮定なしのEnd-to-End方式」の違いを中心に紹介する。なお、類似した方式は同時期に複数発表されてきており、本論文はその代表的な1つであることに注意されたい。

ノウハウが詰まった Hybrid 方式

2020年現在、世の中で使われる音声認識システムは、Hybrid方式と呼ばれるモデル化を広く採用している。Hybrid方式では、音声からテキストへの自動変換問題をいくつかのモデルの組合せにより

実現している。具体的には、音声から音素へのマッピングをモデル化する音響モデル、音素と単語のマッピングをモデル化する発音モデル、そして単語間のつながりをモデル化する言語モデルの3つのモデルから構成され、この構成自体に長年のノウハウが詰まっている。さらに2010年頃からは、個々のモデル化について深層学習の導入が進み、大きく性能改善されたことが音声認識の大きなパラダイムシフトとなり、Hybrid型はすでに1つの完成形の方式となっている。

そんなHybrid方式であるが、いくつかの技術課題があることが知られている。1点目は、音声認識という問題に対して全体最適化されていないということが挙げられる。すなわち、個々に最適化された3つのモデルの組合せは、音声認識の問題に最適であるとは限らないという点である。2点目は、個々のモデル化で、さまざまな独立過程をおいている点である。たとえば音響モデルで用いる隠れマルコフモデルでは、「現在の音素状態は1フレーム前の音素状態にのみ依存する」という独立仮定、言語モデルで用いるn-gramモデルでは、「現在の単語は前の数単語にのみ依存する」という独立仮定をおいている。このような独立仮定はデコーディングの仕組みと相性が良いことから、これまで引き継がれてきたが、それが性能限界を与えていると考えられる。

独立仮定なしの End-to-End 方式

この論文では、前述の2点の課題を解決するために、Listen, Attend and Spell (LAS) と呼ばれ



る End-to-End 方式の手法を提案している。最大の特徴は、音響モデルも言語モデルも発音モデルも使うことなく、音声からテキストへの自動変換問題を LAS という 1 つのモデルで表現している点である (図-1 参照)。そして、その 1 つのモデル内において、独立仮定を一切おこなうことなく全体をモデル化している点も大きな特徴である。

さて、詳細なモデル化の話に入っていこう。LAS では条件付き自己回帰生成モデルにより、音声 (音響特徴量系列) からテキスト (単語系列) への変換を独立仮定なしに End-to-End 方式でモデル化している。具体的には、Listener と呼ばれるリカレントニューラルネットワークに基づく音声エンコーダと、Speller と呼ばれるリカレントニューラルネットワークに基づくテキストデコーダを結合することで、1 つのネットワーク構造により条件付き自己回帰生成モデルを構成している。そして、LAS の面白い点は、Listener と Speller を結びつける Attention の存在である。この Attention の処理は注意機構と呼ばれ、音声の各フレームとテキストの各単語の対応を自動で考慮できる。

モデル全体は、音声とテキストのペアデータから直接最適化でき、具体的には、音声を与えられた際のテキストの条件付き確率の最大化、勾配降下法での学習においては負の対数条件付き確率の最小化によりモデルパラメータを最適化している。一方、音声を与えられたときに学習済みのモデルパラメータを用いてテキストを推定する際は、単語単位の Left-to-Right ビーム探索に基づき、終端記号が出現するまで再帰的に単語を生成することで可変長の

テキストを推定する。

最終的に、最新の Hybrid 方式の音声認識システムの性能には届かないものの、近いところまで End-to-End 方式により到達できることをこの論文では報告している。Hybrid 方式の課題を解決しているのだから、性能改善できるのではないと思われるかもしれないが、理論上は課題を解決できていても、最適化の難しさなどからこの論文の中ではそこまで至らなかったと解釈していただくのがよいだろう。

その後の展開と現状

この論文をスタートとして、独立仮定なしの End-to-End 方式の音声認識技術が大きく進展し、今日では End-to-End 方式が Hybrid 方式を上回る性能を達成してきている。独立仮定なしの End-to-End 方式は最強の方式とも感じられてしまうが、実はまだまだ課題は残っている。現状はモデルへの入力の時点で、すでにヒューリスティックに抽出された音響特徴量系列を前提としているが、音声の波形情報からダイレクトにモデル化する方式の検討がより必要と考えられている。また、現状は 1 つの発話内に閉じて独立性仮定なしに End-to-End でモデル化することがほとんどだが、発話境界を超えてこれまで何を話してきたか、どんなシチュエーション (会話相手、場所など) で発話しているか、などまで含めたモデル化の検討は不十分である。このような未解決の課題に対して、今後どのような技術的ブレークスルーが音声認識に対して生み出されていくのか、期待は膨らむばかりである。

(2021 年 1 月 4 日受付)

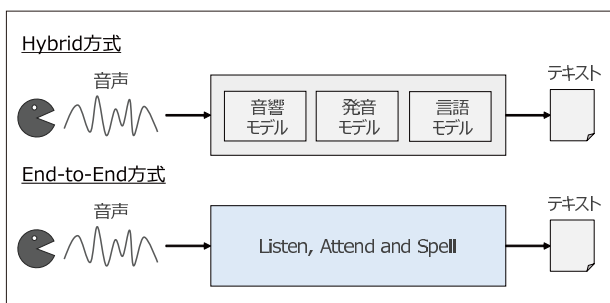


図-1 Hybrid 方式と End-to-End 方式



増村 亮 (正会員)

ryou.masumura.ba@hco.ntt.co.jp

2011 年東北大学大学院工学研究科修士課程、2016 年博士課程修了。博士 (工学)。2011 年日本電信電話 (株) 入社。現在、NTT メディアインテリジェンス研究所特別研究員。音声認識を中心に、音声音響処理、自然言語処理、画像映像処理等のメディア処理全般の研究開発に従事。



VLDB 2020 開催報告

国際会議の概要

国際会議 VLDB (Very Large Data Bases) は、VLDB Endowment^{☆1} が主催する、ACM の SIGMOD (Special Interest Group on Management of Data) と IEEE の ICDE (International Conference on Data Engineering) と並ぶ、データベース分野の主要会議の1つである。日本では過去に東京 (1977年) と京都 (1986年) で開催され、VLDB 2020 は第46回にあたる。

本国際会議への投稿は、研究論文、インダストリアル論文、デモ論文の大きく3つに分かれており、研究論文はさらに Regular Research, Experiment and Analysis, Vision の3つのカテゴリに分かれている。Experiment and Analysis 論文は、既存のアルゴリズムやシステムを網羅的に実験・比較するものであり、再現性を得ることを必須としている。Vision 論文は、その名の通りビジョンに関するものである。なお、Regular Research 論文には、さらに Foundations, Algorithms, System, Information System Architecture という4つの分類があるが、これは査読のためのものである。VLDB 2020 では、投稿数ベースで、各分類の比率はおよそ 3:14:10:2 であった。

VLDB で発表するには、論文誌 PVLDB (Proceedings of the VLDB Endowment)^{☆2} に採録される必要がある。同誌は、研究論文については毎月論文募集を行っている。たとえば VLDB 2020 で発表するには、2019年4月1日から2020年3月1日の間に PVLDB に投稿し採録される必要があり、採録された場合、原則その年の VLDB の発表となる。このようなスタイルは、あまりに VLDB の難易度が上がったため、学術雑誌論文として扱う方が妥当という配慮によるもので、他の国際会議にも広がっている。

開催の準備

筆者らが国際会議 VLDB の日本開催を提案したのは2015年の夏であった。当時は2019年の開催も候補であっ

☆1 <https://www.vldb.org/>

☆2 <https://www.vldb.org/pvldb/>

たが、オリンピック前で東京のホテルの改修が多く、2020年の開催となった。VLDB は8月下旬から9月上旬の開催が原則であるため、8月31日から9月4日に新宿の京王プラザホテルにて、東京パラリンピックと同時開催となった。その時点では、ホテル宿泊費の高騰などの懸念はあったが、まさか現地開催できないことはあるまいと考えていた。

組織としては、本会元会長の喜連川優教授 (東大・NII) に名誉委員長、北川博之教授 (筑波大) に組織委員長をご担当いただき、筆者と Christian S. Jensen (デンマークオーフス大) が共同実行委員長を務めた。プログラム委員長は Magdalena Balazinska (ワシントン大) と Xiaofang Zhou (クイーンズランド大) であった。

2020年の1月頃まではまずまず順調に準備が進んでいたが、パラリンピックの関係で、メイン会場の京王プラザホテルに多くの仮予約が入っているなど、会場のやりくりと交渉に苦労した。ある程度満足のいく会場計画ができたのは2020年3月初めであった。また、横山昌平准教授 (都立大) による、2020年の東京をイメージしたデザインの Web ページ^{☆3} やロゴもできあがった (図-1)。

しかし、COVID-19 によって大きく話が変わることになる。2020年2月頃までは収束を期待していたが、状況の悪化が続いたため、VLDB Endowment との協議によりオンライン開催となった。現状を考えるとその決断は妥当であったと思われる。

オンライン開催が決定したのが2020年4月後半で、それから運営方式の検討やスポンサー規定の見直しなどを行った。オンライン会議では、リアルタイム発表はトラブルのもととなるため、YouTube に事前に発表ビデオを上げておくことにした。また、中国の参加者を対象に bilibili にもビデオを掲載した。

一番の問題は時差への対応であった。日本時間での開催は米国の参加者が多いことを考えると無理があり、日本の夕方から深夜の開催ならばなんとか全世界で見られるが、発表件数が十分さばけないという問題があった。結局、ほぼ24時間のプログラムとして、各論文を別々の時間帯で2回発表させることにした。ただし、発表時にはまずビデオを再生し、質疑応答だけ著者に Zoom で対応してもらった (質疑応答は1回のみ対応でも可とした)。24時間のタイムチャートを図-2に示す。

☆3 <https://vldb2020.org/>



図-1 VLDB 2020 のバナー

オンライン会議の運営のため、日本からは技術委員長の宮崎純教授(東工大)にご尽力いただいた。特にネットワークの冗長化などによる安定した運営が課題であったが、大きなトラブルなしに会議が開催できた。VLDB 2020の登録者は、会議終了時点で4,723名であった。ただし、実際のセッションには登録者ほどには参加者がいないことも多々あり、これは24時間体制と、発表を録画提供していたことによると思われる。また、Zoomによるスポンサーブースを設けたが、集客は十分でなく、オンライン会議の難しさを痛感した。

会議の内容

基調講演の1つ目はDan Olteanu教授(チューリッヒ大)によるThe Relational Data Borg is Learningと題した、リレーショナルデータベース上での機械学習に関する講演であり、ビッグデータに基づく機械学習を各段にスケールアップするアプローチの解説があった。2つ目はJulia Stoyanovich(ニューヨーク大)によるResponsible Data Managementであった。近年、人工知能による判断の公平性・公正性の問題が議論されているが、そもそもデータ管理の時点で対応すべきであり、データベース研究としてどう取り組むかという話であった。3つ目は喜連川優教授によるOut-of-order Execution of Query Processing and New Advances in COVID-19 Informationであった。アウトオブオーダー型と呼ばれる新たなDBMSのアーキテクチャとそのインパクトの紹介に加え、情報学の立場から日本におけるCOVID-19への取り組みの話があった。

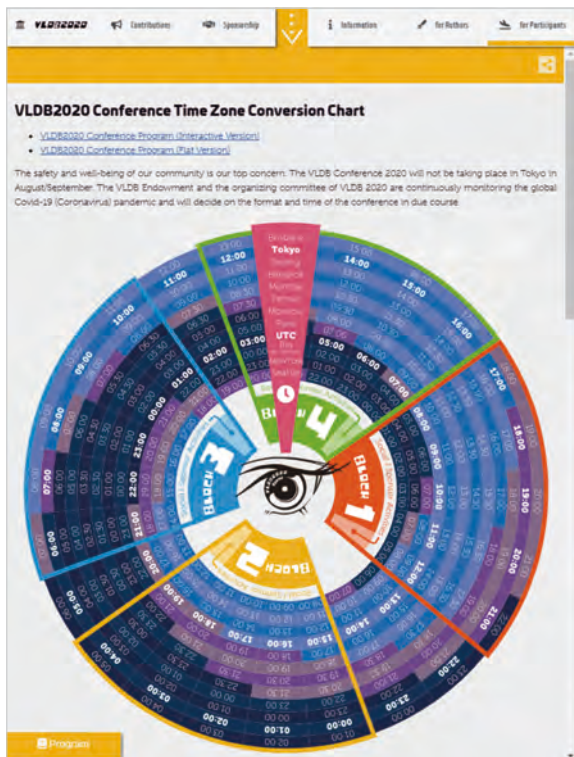


図-2 タイムチャート
(https://vldb2020.org/program_timetable.html)

研究論文の分野ごとの内訳を図-3に示す。アルゴリズムの面では、大規模なグラフ・ネットワークの間合せや分析技術の研究が依然としてホットである。システムの面では、マルチコア、大規模な主記憶、不揮発性メモリなどの新しいハードウェア環境のためのDBエンジンの研究が進んでいる。機械学習・人工知能の研究も盛り上がっているが、VLDBクラスになると単に機械学習を適用したという研究はなく、大規模スケールでの機械学習や、DBMSの性能向上のための機械学習の活用など、なるほどと思わせる論文が多い。

VLDBの場合、研究論文の件数はその年のPVLDBの採録数で決まるが、VLDB 2020は207件であり、過去最大のVLDB 2015(ハワイ)の1.3倍であった。これは日本での会議にいかに関心を持たれていたかを意味する。筆者自身も多くの研究者から、2020年はぜひとも日本を訪れたいとのコメントをいただいていた。

会議運営の感想

東京での会議を提案したときには、まさかこのような結果になるとは思いもよらなかったが、すべての研究発表を実施でき、また、運営面でも赤字にならなかったことで、最低限の条件は達成できたといえる。24時間の運営は苦肉の策であったが、参加者のメリットは大きかったと考える。一方、オンライン会議の運営では特定の人に仕事が集中する難しさがあった。また、日本の多くの方々、特に若手研究者に会場に参加していただき最先端の研究を味わってもらおうということが叶わなかったのは残念である。運営にご尽力いただいた方々と、ご支援いただいたスポンサーの皆様には深く感謝する次第である。

VLDB 2021はコペンハーゲンでの開催が予定されている。現時点ではオンラインとリアルなハイブリッド開催が計画されていると聞く。この困難な時代に国際会議を運営し、学問を進めていく意義は重要であり、日本からも多くの投稿を期待したい。

石川佳治
(名古屋大学)

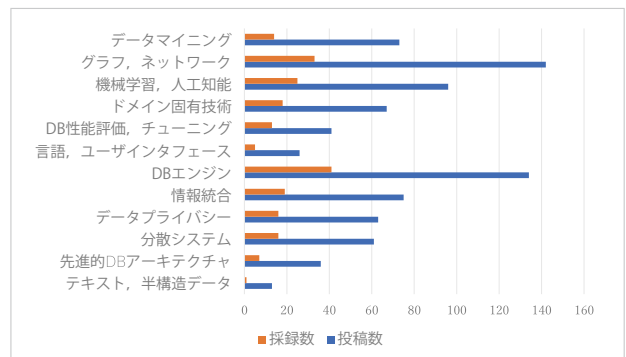


図-3 研究論文の投稿数と採録数

「情報教育課程の設計指針」解説



萩谷昌己 | 東京大学



背景

2020年9月25日に日本学術会議より報告「情報教育課程の設計指針—初等教育から高等教育まで」¹⁾が公表された。この報告の策定にあたったのは情報学委員会のもとにある情報学教育分科会である。筆者はその分科会の委員長を9月末まで務めた。本稿では、この報告を策定した分科会の委員長として、この報告に関して解説させていただきたい。以下では、この報告を「設計指針」と記す。

この報告に先立って、2016年3月23日に日本学術会議より報告「大学教育の分野別質保証のための教育課程編成上の参照基準 情報学分野」²⁾が公表されている。こちらの報告は、情報学委員会のもとにあった情報科学技術教育分科会が策定した。情報科学技術教育分科会は情報学教育分科会の前身の分科会であり、こちらの分科会の委員長も私が務めていた。名称変更の理由として、情報学分野の参照基準が公表されたことを踏まえ、情報学という学問に則して情報教育の検討を行おうという意図があった。なお、筆者は第22期と第23期の6年間、日本学術会議の会員として情報科学技術教育分科会の委員長を務め、第24期の3年間は連携会員として情報学教育分科会の委員長を務めた。なお、2020年に始まった第25期では、日本学術会議の在り方自体が問わ

れていることは読者もよくご存じであろう。

2つの報告ともに、日本学術会議の協力学術研究団体である本会の情報処理教育委員会の多大な協力を得て策定された。筆者は2016年5月から2020年5月まで情報処理教育委員会の委員長も務めており、分科会と情報処理教育委員会の協力関係の恩恵にあずかることができた。

特に「設計指針」は、情報処理教育委員会の委員であった久野靖氏が中心になって策定された。久野靖氏には情報学教育分科会の特任連携会員もお願いし、日本学術会議における査読の過程においても、指摘事項への対応に本当に心血を注いでいただいた。ここに改めて感謝の意を表したい。

さて、日本学術会議による分野別の参照基準は、大学（学士）専門課程の分野別質保証のために策定されてきたもので、すでに30以上の分野の参照基準が策定され公表されている。分野別の参照基準では、その分野の定義と固有の特性、その分野を学ぶすべての学生が身に付けることを目指すべき基本的な素養、学修方法および評価方法に関する基本的な考え方、そして、専門性と市民性を兼備するための教養教育が述べられる。最後の項目では、その分野を専門に学ぶものが身に付けるべき教養について述べられる。情報学分野の参照基準においても、これらの項目について述べられているが、さらにその次

に「専門基礎教育および教養教育としての情報教育」という項目が追加されている。この項目が「設計指針」につながったのであるが、この項目について述べる前に、情報学分野の参照基準の全般について復習したい。

まず、情報学分野の参照基準では、情報学を「情報によって世界に意味と秩序をもたらすとともに社会的価値を創造することを目的とし、情報の生成・探索・表現・蓄積・管理・認識・分析・変換・伝達にかかわる原理と技術を探求する学問」と定義している。意味と秩序の創出および社会的価値の創造という学問の目的を述べているところは、他の分野にない特徴である。学問の目的を述べることにより、目的に沿った諸活動を情報学の活動としても積極的に認めようという、情報学の広がりやを宣言しているとも考えることもできるだろう。また、目的の次には、情報学が情報のあらゆる側面を対象としていることを述べており、情報学の普遍性ととともに、情報学があらゆる分野の基盤の1つとして位置付けられることを示唆している。そのように他の諸分野において共通して必要な学問を「メタサイエンス」と呼ぶことがあるが、数学や統計学と同様に、情報学もこの意味でメタサイエンスの1つとして位置付けられる。情報学分野の参照基準においても以下のように述べられている。

情報学の中核部分が諸科学に対する『メタサイエンス』であるという考えがある。メタサイエンスとは諸科学全体を覆うサイエンスを意味している

この考え方が、後述するように「設計指針」の基礎となっている。

情報学分野の参照基準では、情報学を上述したように広がりのある学問分野と位置付けながらも、学士課程の専門教育の観点、すなわち、情報学の専門家を養成するという観点に立って、情報学全体では

なく情報学の中核部分を体系化している。情報学の中核部分は、以下の5つの分類にしたがって定義される。これらは、情報学を学ぶすべての学生が身に付けることを目指すべき基本的な素養のうち、獲得すべき基本的な知識と理解をまとめたものであり、括弧の中は「設計指針」の中で参照される際に用いられる略称である。

- ア 情報一般の原理（情報一般）
- イ コンピュータで処理される情報の原理（機械情報）
- ウ 情報を扱う機械および機構を設計し実現するための技術（情報処理）
- エ 情報を扱う人間社会に関する理解（人間社会）
- オ 社会において情報を扱うシステムを構築し活用するための技術・制度・組織（システム）

ここではこれらの5つの分類についてさらに詳しく述べることはしないが、社会情報学などの情報社会を扱う学問分野も情報学の中核部分に含まれていることに注意してほしい。情報学分野の参照基準では、情報社会を扱う分野と、コンピュータ科学を中心とする理系と考えられている諸分野の上に、さらに「情報一般の原理」が置かれ、情報学の中核部分が1つの学問分野として体系化されている。

ここでようやく、「設計指針」を読むための予備知識が揃ったことになる。「設計指針」の冒頭は以下のように始まる。これがまさに「設計指針」を策定した理由であり、「設計指針」の内容をも示している。

情報学分野の参照基準でも述べられているように、情報学はメタサイエンス（複数分野の科学に共通して必要な学問）として、すべての諸科学の基盤の1つと考えられ、市民の一人一人が情報技術に関する知識を背景として、情報社会の制度や情報倫理に関する見識を有

していることが望まれる。そのために情報学分野の参照基準では、情報学以外の専門課程における基礎教育（専門基礎教育）、さらに初等中等教育から大学の共通教育に至る教育課程における情報教育について述べているが、そこでは基本的な考え方を示すにとどまっており、各教育段階での教育内容について詳細な検討を行っているわけではない。

すなわち、「設計指針」では、各教育段階での情報教育の内容について詳細な検討が行われている。さらに、「設計指針」の目的が述べられている以下の箇所を引用したい。

本報告は、情報教育の共通の物差しとして、各学校等の教育現場において情報教育に携わる者、情報教育を設計・評価する者が、自らの学校段階の情報教育と、隣接する学校段階や、大学での専門分野における情報教育の関係について検討する際の指針として、また、情報教育全体（もしくはその一部）を設計する者が体系化の手段として用いることを期待する。

ここまでで、「設計指針」を策定した背景、理由、内容、目的について分かっていたことと思うが、さらに「設計指針」と情報学分野の参照基準との違いについて述べておきたい。情報学分野の参照基準は学士課程の専門教育を対象としている。すなわち、情報学を専門とする学生に対する学士課程（学部レベルの教育課程）を定義している。これに対して、「設計指針」は初等教育（小学校の教育）から高等教育（大学の教育）までを対象としている。ここで高等教育とは、すべての分野における専門教育を意味している。情報学の専門教育もこの中に含まれるが、それはほんの一部に過ぎない。「設計指針」で述べられている情報教育は、情報学の専門教育に

接続してはいるものの、それは数多くある専門教育の1つとしてでしかない。

上述したように、情報学分野の参照基準の中で、最後の項目「専門基礎教育および教養教育としての情報教育」が、「設計指針」に直接的に関連している。この項目では、教養教育および各分野の専門基礎教育における、情報学の教育の重要性について述べられている。ここで専門基礎教育とは、それぞれの専門分野の課程において行われる基礎教育を意味している。さらに以下のように、情報学分野の参照基準が、教養教育と専門基礎教育だけでなく、初等中等教育における情報教育を先導すべきことが述べられている。

ここで特筆すべきは、大学一般情報教育も高等学校普通教科情報科も、理系の情報学のみならず、情報社会の制度や情報倫理など、文系の情報学を含んでいることである。すなわち、初等中等教育から大学教養教育に至るまで、情報学は、文系と理系にまたがる広い分野として認識されて教育されているのである。したがって、本参照基準が定める情報学の中核部分は、初等中等教育から大学教養教育に至るまでの情報教育に対する基礎を与えており、将来にわたって、情報教育を先導する役割も担っている。

以上の背景のもとで「設計指針」は策定された。以下で述べるような枠組みのもとで、初等教育から高等教育までの情報教育を一貫通貫で記述した文書は、これまでなかったといっただろう。

検討の枠組み

情報教育の共通の物差しの策定にあたって、当然ながら情報学分野の参照基準がその土台とされた。すなわち、情報学分野の参照基準が定める知識・能

力のうち、大学教養教育および専門基礎教育として相応しいものが抽出された。さらに、「学士課程教育の構築に向けて（答申）」³⁾（以下「学士力」として参照）が参考にされた。「学士力」は、学士課程に共通する知識・理解・スキル・態度・志向性を示した文書である。これらを併せることにより、学士課程における情報教育の到達点を定めることができる。学士課程の到達点が定めれば、そこから逆算して、学習指導要領などを参照しながら、高等学校、中学校、小学校における教育課程を検討することができる。

いささかテクニカルな話になるが、学士課程の到達点を検討するにあたっては、ジェネリックスキルが重要な検討対象となった。分野別の参照基準では、その分野を学ぶすべての学生が身に付けることを目指すべき基本的な素養として、獲得すべき基本的な知識と理解、および、獲得すべき能力が述べられる。基本的な知識と理解は、情報学の中核部分の5つの分類ア～オとしてすでに紹介した。獲得すべき能力はさらに、獲得すべき専門的能力（各分野に固有の能力）とジェネリックスキルに分けられる。情報学分野の参照基準では、ジェネリックスキルとして、以下のア～カが定められている。括弧内は「設計指針」で用いられている略称である。

- ア 創造性（創造性）：創造力・構想力・想像力
- イ 論理的思考・計算論的思考（論理）：論理的思考能力・論理的緻密さ・演繹する能力・概念化・モデル化・形式化・抽象化を行う能力
- ウ 課題発見・問題解決（問題解決）：問題発見能力・問題解決能力・システム思考・クリティカルシンキング
- エ コミュニケーション（コミュ）：コミュニケーション能力・プレゼンテーション能力
- オ チームワーク・リーダーシップ・チャンス活用（チーム）：協調性・リーダーシップ・ストレス耐性

- カ 分野開拓・自己啓発（主体性）：主体的に学習する能力・融合する力・関連付ける力

一方、「学士力」では、学士課程共通の学習成果に関する参考指針として、Ⅰ．知識・理解、Ⅱ．ジェネリックスキル（汎用的技能）、Ⅲ．態度・志向性、Ⅳ．総合的な学習経験と創造的思考力の4分類があげられている。ジェネリックスキルという言葉の意味合いが異なっていることに注意してほしい。Ⅱ～Ⅳはすべて、上記の情報学分野の参照基準のジェネリックスキルに対応している。「設計指針」では、Ⅱ～Ⅳに対応する能力として、上記のジェネリックスキルのうちから、学士として社会に出た段階で専門分野にかかわらず共通に必要なとされる水準までが取り入れられた。

なお、「学士力」のⅠに対応する知識・理解としては、情報学分野の参照基準における基本的な知識と理解（5つの分類ア～オ）から、すべての大学生が学ぶべきだと考えられる情報学の内容が取り入れられた。

ここで参考のために、情報学において獲得すべき専門的能力についても掲載しておく。括弧内は略称である。

- ア 情報処理・計算・データ分析（情報処理）
- イ システム化（システム）
- ウ 情報倫理・情報社会（倫理社会）

以上のようにして、学士課程の到達点が定められた後、初等中等教育については、学習指導要領およびその解説などが参照された。初等中等教育では、中学校の技術科（情報分野）と高等学校の情報科が、専門に「情報」を扱う科目として設定されているが、情報教育は決してこれらの科目に限定されるものではない。小学校では「情報」を専門に扱う教科は存在せず、プログラミング等の「情報」にかかわる教育が、既存の教科および総合的な学習の時間におい

で行われている。

以上の枠組みのもとで「設計指針」では、次節で紹介するように、情報教育の学習内容が11カテゴリにまとめられている。これらの内容は、決して現行の情報教育をそのまま反映したものではない。かといって、非現実的な学習目標を設定したものでもなく、抽象的な理想論を述べたものでもない。現行の学習指導要領を踏まえつつ、より充実した情報教育を指向した結果となっている。したがって、前述したように「設計指針」は、情報教育の共通の物差しとして活用するための実用的な文書と位置付けることができる。一方、分野別の参照基準では、各分野における教育の理想像が述べられているといっても過言ではない。当初、「設計指針」は「情報教育の参照基準」として、分野別の参照基準の1つとしての公表が計画されていたが、日本学術会議における査読の過程の中で、分野別の参照基準とは異なる種類の文書として公表すべきと結論付けられ、タイトルもその内容により則したものに変更された。

11 カテゴリと学校段階・科目

「設計指針」では、情報教育の学習内容がA～Kの11カテゴリにまとめられている。11カテゴリのうち、A～Hの8カテゴリは、狭い意味で情報教育と一般に捉えられているものであり、これらはさらに以下の5つの領域①～⑤に分類される。I～Kの3カテゴリは、前述したジェネリックスキルから成っており、以下の⑥にまとめて示されている。これらは後述するように、ジェネリックスキルを中核とする「総合情報処理能力」と位置付けることができる。以下では、①～⑥のそれぞれに属する11カテゴリも示されている。表-1も参照されたい。

- ① 情報とコンピュータの仕組み：A. 情報およびコンピュータの原理
- ② プログラミング：C. モデル化とシミュレーション・最適化, E. 計算モデル的思考, F. プログラムの活用と構築
- ③ 情報の整理や作成・データの扱い：B. 情報

■表-1 情報教育における分野の分類

領域	カテゴリとその記号	情報学固有の知識	ジェネリックスキル	専門的能力
情報とコンピュータの仕組み	A. 情報およびコンピュータの原理	情報一般, 機械情報, 情報処理, 人間社会, システム	論理, 問題解決	倫理社会, システム
プログラミング	C. モデル化とシミュレーション・最適化	情報一般, 機械情報, システム	創造性, 論理, 問題解決	情報処理, システム
	E. 計算モデル的思考	情報一般, 機械情報	創造性, 論理, 問題解決	情報処理, システム
	F. プログラムの活用と構築	機械情報, 情報処理, システム	論理, 問題解決	情報処理, システム
情報の整理や作成・データの扱い	B. 情報の整理と創造	人間社会	創造性, 論理, コミュ, 主体性	
	D. データとその扱い	情報一般, 機械情報, 情報処理, 人間社会	創造性, 論理, 問題解決	情報処理, システム
情報コミュニケーションや情報メディアの理解	G. コミュニケーションとメディアおよび協調作業	情報一般, 機械情報, 人間社会	創造性, 問題解決, コミュ, チーム	倫理社会
情報社会における情報の倫理と活用	H. 情報社会・メディアと倫理・法・制度	機械情報, 人間社会, システム	論理, 問題解決, コミュ, チーム	システム, 倫理社会
(総合情報処理能力)	I. 論理性と客観性	機械情報, 人間社会, システム	論理, 問題解決, コミュ, チーム	倫理社会
	J. システム的思考	人間社会, システム	問題解決, コミュ	システム
	K. 問題解決		問題解決, チーム, 主体性	システム

解説
Article

- の整理と創造, D. データとその扱い
- ④ 情報コミュニケーションや情報メディアの理解 : G. コミュニケーションとメディアおよび協調作業
- ⑤ 情報社会における情報の倫理と活用 : H. 情報社会・メディアと倫理・法・制度
- ⑥ ジェネリックスキル (総合情報処理能力) : I. 論理性と客観性, J. システム的思考, K. 問題解決

各カテゴリは3~5個の項目から成り, そのそれぞれは4つのレベルに分けられている. 各レベルには, そのレベルの内容を扱うことが想定される学校段階と科目が指定される. たとえば, カテゴリ「A. 情報およびコンピュータの原理」の2つの項目A1とA4は以下のようなものである.

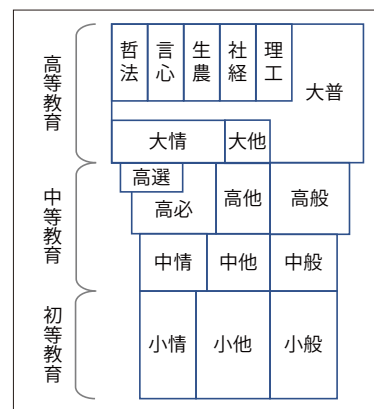
- A1. 情報が持つ特性やその表現方法に関する知識・理解 (知識: 情報一般), (知識: 機械情報)
L1: 情報 (知らせ) とは何かということ (小情)
L2: 情報を外部化 (書き記すなど) により記録・表現できるということ (小情)
L3: デジタル/アナログ, 二進表現, 多様な情報の表現方法 (高必)
L4: 個体や組織とそれらにとって情報のやりとりが持つ意味 (大情)
- A4. コンピュータやネットワークにまつわるセキュリティの概念やそのための技術に関する知識・理解 (知識: 機械情報), (知識: 人間社会), (知識: システム), (専門: システム), (専門: 倫理社会)
L1: コンピュータやネットワークにまつわる「安全」の意識と基本知識 (小情)
L2: マルウェア, 不正アクセス等のセキュリティの基本的な知識・理解 (小情)
L3: 情報セキュリティの考え方・原理と暗号など

- のセキュリティ技術の理解 (高必)
- L4: 情報社会での情報技術関連のリスク要因・リスク評価の知識・理解 [哲法][社経]

ここで, (知識: 情報一般) は情報学分野の参照基準における基本的な知識と理解の (情報一般), (専門: システム) は専門的能力の (システム) を参照している.

各レベルにおける学校段階と科目は, 以下のよう
に定義されている (図-1).

- (小情) (中情) — 小学校で情報教育として, また中学校で技術・家庭科の技術分野で学ぶ内容. 小学校・中学校に情報科が設置された場合はそこで扱うと想定される
- (小他) (中他) — 前項以外のさまざまな科目において学ぶ内容
- (小般) (中般) — 特定の科目内でなく, 小学校・中学校の教育全体として学ぶ内容
- (高必) — 高等学校の情報科の必修科目を通して全員が学ぶことが望まれる内容
- (高選) — 選択科目を通して高等教育に進む生徒が学ぶことが望まれる内容
- (高他) — 前項以外の科目において学ぶ内容
- (高般) — 特定の科目内でなく, 高等学校の教育全体として学ぶ内容
- (大情) — 大学共通教育 (主に1年次) の中で,



■ 図-1 学校段階と科目

主として情報科目として学ぶことが想定される内容

- (大他) — 大学共通教育 (主に1年次) の中で、主として情報の科目以外の科目として学ぶことが想定される内容
- (大普) — 普遍的事項。この内容は学士取得までに卒業研究やゼミなどを通じて身に付けていくことを想定している。この内容も、どの専門でも共通であるが、ただし具体的な文脈 (取り扱うテーマや細かいスタイルなど) は分野ごとに異なる
- [専攻グループ名] — 専門基礎教育や専門教育において、各専攻分野ごとの題材で学ぶ内容。これは、専攻分野ごとに題材や扱い方が違うことを想定する。本報告では専攻分野を5つのグループに大別して整理している

大学の専門分野は、各分野で行われている情報教育の類似性に基づいて、以下のように5つのグループに分類されている。なお、この分類は、決して学問分野を分類するというものではなく、類似の情報教育が行われているかによって、専門分野を大まかに分類したものにすぎない。

- [哲法] — 哲学、法学、政治学等
- [言心] — 言語学・地理学・心理学等
- [生農] — 生物学・農学・医学等
- [社経] — 社会学・経済学・経営学等
- [理工] — 理学・工学等

専門基礎教育や専門教育における情報教育は、それぞれの専門分野で行われるものであり、専門分野の教員が教えることが想定される。しかしながら、特に専門基礎教育における基礎的な内容に関しては、他の分野の学生にも開かれていることが望まれるだろう。

さて、上述した11カテゴリは、かなりの時間を

かけて統合・分割を繰り返しながら、最終的な形に落ち着いたものである。「設計指針」でも以下のように述べられている。

初等中等教育および高等教育における共通教育ならびに専門基礎教育までを合わせ、情報教育において単独の概念として取り扱うことが適当と考える範囲を想定した上で、1カテゴリの記述が大きくなりすぎないように分割し整理したものである。

2019年5月18日には公開シンポジウムを開催し、関連学会の有識者も招いて広く意見を募り、寄せられた意見をもとに改訂を行った。このような改訂を繰り返した結果として11カテゴリが得られた。

ジェネリックスキル (総合情報処理能力) は3つのカテゴリI~Kから成り、各カテゴリはさらに3~4の項目に分かれている。日本学術会議の査読の過程において、この分類は細かすぎるという批判があった。しかしながら、I~Kは一般的なジェネリックスキルというよりも、ジェネリックスキルを中核とする「総合情報処理能力」として位置付けることができる。これらの能力の分類は、情報教育の内容を精査し整理することにより自然と得られたものである。

一方、コミュニケーション能力や主体性のような一般的なジェネリックスキルは、I~Kに限らず他のカテゴリにも関連している。「設計指針」では、各カテゴリの各項目に情報学分野の参照基準における各ジェネリックスキルが対応付けられている。以下はその例である。(汎用: コミュ) は、ジェネリックスキルの (コミュ) を示している。

- G3. 協調作業やそのためのコミュニケーション／プレゼンテーションの技能 (汎用: コミュ), (汎用: チーム)
- L1: 「一緒に~する」「分担して~する」をコミュ

- ニケーションできる (小般)
- L2: 共同作業のためのコミュニケーションに際して合意・確認が取れる (中般)
- L3: 共同作業の目的や進め方を集団の前でプレゼンテーションできる (高必)
- L4: 目的のために誰とコミュニケーションするか計画し実践できる (大普)

この章のまとめとして、「設計指針」の表-1を引用する。より詳しくは、「設計指針」そのものを参照していただきたい。

活用の可能性

「設計指針」は、さまざまな場面で活用されると確信している。その典型例は高大接続であろう。大学側は入学する学生が高等学校で何を学んだかを把握することができ、高等学校側は大学における教育を把握することにより、大学が何を期待しているかを推測することができる。大学入試においては、さまざまな形で活用されるだろう。筆記問題の作成以外にも、AO入試における判断基準として用いることができる。

同様に、「設計指針」は中学校と高等学校の接続においても有用である。特に、中学校の技術科(情報分野)と高等学校の情報科の関連が明確になるだろう。その結果として、高等学校に入学した段階で

の生徒の知識や能力の格差が低減されることを願っている。

小学校ではプログラミング教育が始まっているが、教育の目標が設定されることにより、カリキュラムや教材の開発が進展するだろう。

各学校段階における教科間の関係を把握する際にも有用である。たとえば、高等学校の情報科が他の教科に何を期待しているかが明らかとなっている。そして、いうまでもなく、2020年に小学校から開始された学習指導要領の次の学習指導要領の設計に活用されることを期待している。

今後、情報教育の共通の物差しとして、策定者の期待しないような形で活用されることを望んでいる。

参考文献

- 1) 日本学術会議：報告「情報教育課程の設計指針—初等教育から高等教育まで」令和2年(2020年)9月25日, 日本学術会議情報学委員会情報学教育分科会.
- 2) 日本学術会議：報告「大学教育の分野別質保証のための教育課程編成上の参照基準 情報学分野」平成28年(2016年)3月23日, 日本学術会議情報学委員会情報科学技術教育分科会.
- 3) 中央教育審議会：学士課程教育の構築に向けて(答申), 2008年12月.

(2021年1月5日受付)

萩谷昌己(正会員) hagiya@is.s.u-tokyo.ac.jp

東京大学大学院情報理工学系研究科コンピュータ科学専攻教授。2016年より2020年まで本会情報処理教育委員会委員長。2020年より本会副会長。2011年より2017年まで日本学術会議会員。2017年より日本学術会議連携会員。



今月の会員の広場では、1月号へのご意見・ご感想を紹介いたします。まず、巻頭コラム「情報と食の未来」については、以下のようなご意見・ご感想をいただきました。

■共感できた。 (匿名希望)

特別解説「HER-SYSはなにが問題だったか」については、以下のようなご意見・ご感想をいただきました。

■現実の問題の失敗の理由を明確に分析している。 (風間一洋)

■ICTの分野以外の方を取り上げることは良いことだと感じている。 (河村 悟)

■要件定義の難しさや現場の状況が正しく伝わらない点など、分野が違うもののリアルに感じられて興味深かった。 (大江秀幸)

■コロナ禍での保健所での情報システム担当者の奮闘記とも言える内容であり、日本の今の保健行政の問題点(予算や人員の不足など)を浮き彫りにしていると思いました。 (松浦満夫)

■ニュースにはない専門的な解説で、HER-SYSの問題点を大変よく理解できた。 (角田洋太郎)

■リアルで素晴らしく良かったです。 (佐藤 哲)

■「積極的疫学調査として関係する情報をなんでも集めてよい」となりがちなところを「要配慮個人情報」として適正な取り扱いがなされているかを慎重に確認した上で対応していただいていることに感銘を受けました。同時に、自分が同じような状況に置かれた場合に注意しなくてはと自戒しました。 (大森麻理)

■事実に基づいたきわめて重要な提言となっており、ぜひ平井卓也デジタル改革担当大臣に読んでいただきたいと思った。 (伊藤雅樹)

■ドキュメンタリー形式のように分かりやすい構成で、システムに対する期待と、実際の実装の課題、改善の流れを読み取ることができ、非常に興味を掻き立てられた。 (佐伯嘉康)

■大変勉強になりました。特に、仕様が現場のニーズと乖離してしまった根本原因が、厚労省内の感染症専門職員の激務にあったことは、もっと世間に知られてもいいのではないかと思います。 (服部充洋)

特別解説「あなたにとって『情報』は入試科目ですか?の歴史」については、以下のようなご意見・ご感想をいただきました。

■面白かった。このような、社会とのかかわりや関係について議論できるような記事を今後も期待したいと思っています。 (平澤将一)

特集「AI人材教育」については、以下のようなご意見・ご感想をいただきました。

■高校・大学でどのような情報・AI教育がされているか、数多くの事例を知ることができ有意義だった。「情報」を高校で学び「AI」を大学一般教養で学んだ若手との、世代ギャップを埋めるのにも役立ちそうだ。 (金子雄介)

■「滋賀大学におけるAI人材教育」と「早稲田大学におけるAI人材教育」を特に興味深く読みました。前者では日本でのデータサイエンス教育の先駆的な存在としてのデータサイエンス学部の取り組みが新鮮に映りました。また、後者ではデータ科学センター設置による全学的なデータサイエンスの研究・教育が進められていることが印象的に感じました。 (松浦満夫)

■AIについての記事がとても面白かったです。 (西川雄喜/ジュニア会員)

「4. 早稲田大学におけるAI人材教育」

■総合大学(早大)におけるAI人材育成のための取り組みとして全学的組織である「データ科学センター」を設置した経緯やそこでの実践についての記事であり、よく検討されており参考になった。 (丹羽邦彦)

連載「情報の授業をしよう!!:科目「情報セキュリティ」の授業実践」については、以下のようなご意見・ご感想をいただきました。

■自分の実践に役立つ。 (匿名希望)

教育コーナー「ペタ語義:情報の専門家とICT苦手教員の間に潜む間隙」については、以下のようなご意見・ご感想をいただきました。

■経験則のみで語られているので興味が持てない。 (匿名希望)

■私も「カメラ」という表現を使ってしまうと思いました。友人や同僚と話している分には通じる言葉で話していても問題ありませんが、教えるとなると正しく用語を使い、適切な操作を伝える必要があります。自分の常識が常識でない方に教える心構えを再認識いたしました。 (匿名希望)

オンライン版で読みたい記事、期待するコンテンツについて以下のようなご意見やご要望をお寄せいただきました。

■これまで通り、最先端のテーマを取り扱っていただけると大変勉強になります。 (遠山紗矢香)

■期待はしますが、今のところ、オンライン版の方が良かったことは感じられていません。通常、オンライン版のメリットで感じられるのは検索機能のため、毎月の会誌ごとではなく、論文誌などの単位のほうがメリットは感じられるのかもしれませんが、逆に言うと、正直なところ現状では会誌は印刷版を望んでいます。 (佐藤 哲)

■プログラムやシステムなどのデモを動画で配信できれば面白いと思います。 (川口雅司)

■プログラミング技法, 人工知能など。 (巫召鴻)

■実際に「動く」ものは見てみたいと思います。 (大江秀幸)

■産学連携の一環として, 社会人博士課程についての記事が読みたい。 (木村良一)

■オンライン版(情報学広場)での会誌閲覧のユーザ体験については, 改善の余地があると考えます。全体版のファイルサイズが大きく(今月は70MB), タブレット端末で閲覧するとレンダリングが重く, 非常にストレスを感じる(ザッピングができないのが辛い)。個別記事のダウンロードが記事単位になっており, 特集やコーナーを通して読むのに煩雑な操作が発生する。特集, 各コーナー単位でファイルがまとまっていると, 非常に読みやすい。個別記事のダウンロードは, タイトルだけで内容が掴めない記事があるので, タイトルを工夫するか, 概要を表示してほしい。特にタイトルが毎月同じ連載物に顕著です。たとえば「先生, 質問です!」のコーナーは毎月質問が変わるが, 現在の仕様では, 実際にファイルを開いてみるまで内容が分かりません。もちろん個人の閲覧環境のすべてに対応することは不可能ですが, 2020年秋に発売された比較的新しい機体でもレンダリングの遅さを感じており, 小さくない範囲のタブレット端末でユーザ体験が損なわれているのではないかと推測しています。 (中川 岳)

会誌の内容や今後取り上げてほしいテーマに関して, 以下のようなご意見やご要望をお寄せいただきました。今後の参考にいたします。

■音楽や演劇と情報処理の関係など。 (巫召鴻)

■「HER-SYS はなにが問題だったか—先行導入, 本導入, 改修提案を振り返って—」のような現在の問題に対する「特別解説」記事は, 一般公開時期を早めて会誌発行日から読めるようにすべきではないのか? 日本学術会議の問題などで, 「一般国民から」学会の存在意義が疑問視されている情報を踏まえて, ぜひ非会員へのタイムリーな情報発信として検討していただきたい。あと, 会誌を

読みながら入力すると, タイムアウトするのかエラーになる問題は, そろそろちゃんと解決していただきたい。 (風間一洋)

■インターネットによって生活が一変し, すこぶる利便性が高まったが, 反面安易に結果を求める風潮が強まっていることに若干の危惧を感じている。このあたりについての関係者(特に教育に携わっている方)のご意見を賜りたいです。 (河村 悟)

■小学生の子供がおりますので, 教育関係のコンテンツは楽しみに読んでいます。 (大江秀幸)

■モニタアンケートのメールでの回答書式が今回からなくなったようだ。一方で, Web サイトでの回答フォームは, 記入途中で保存して後で再開する機能がない。つまり Web サイトに回答を入れるには, 別のどこかに回答を用意しておいて, 一気に入れなければならない。その「別のどこか」として, これまではメールでの回答書式をメモ代わりにしていたが, それもできなくなってしまった。不便極まりない印刷イメージの学会誌 PDF もそうだが, 相変わらず質問 [9] (どちらの媒体で記事をお読みになりましたか?) にハイブリッドの選択肢もないし, 読者やモニタに対するサービスは悪化の一途である。読者やモニタの立場に立って(一度, 自分で回答を入れてみたりして), すべてを見直すことを強く要望する。記事内容は充実しているのに, 大変残念である。 (伊藤雅樹)

■各分野持ち回りで最新のサーベイ記事を掲載してほしい。会誌の内容ではないですが, アンケートの記入に長時間かけると, エラー表示になるのは改善してほしい。丁寧に書いて「エラーです」と言われると非常に気持ちが萎えます(今回も一度書き直しました)。おそらくセッションの時間切れだと思われませんが……。 (中川 岳)

■PDF 版会誌はスマートフォンだと読みにくいのでレイアウトを改良してほしい。 (角田洋太郎/ジュニア会員)

【本欄担当 若林 啓・村上洋一/会員サービス分野】

これらのコメントは Web 版会員の広場「読者からの声」<URL : <https://www.ipsj.or.jp/magazine/dokusha.html>>にも掲載しています。Web 版では, 紙面の制限などのため掲載できなかったコメントも掲載していますので, ぜひ, こちらもご参照ください。会誌や掲載記事に関するご意見・ご感想は学会 Web ページでも受け付けております。今後もより良い会誌を作るため, ぜひ皆様のお声をお寄せください。

皆様にとって会誌をより役立つものとするため,

- ・記事に対する感想, 意見
- ・記事テーマの提案
- ・会誌または学会に対する全般的な意見, 提言
- ・その他, 情報処理技術についての全般的な意見, 提言

など自由なご意見, ご感想をお待ちしております。

なお, 「道しるべ」については

<URL : <https://www.ipsj.or.jp/magazine/sippitsu/michishirube.html>> で

これからのテーマ案を募集しており, いただいたご意見をまとめております。

※ご意見, ご感想を会誌に掲載させていただいた方には薄謝または記念品を進呈いたします。

掲載に際しては, 編集の都合上, ご意見に手を加えさせていただくことがありますので, あらかじめご了承ください。

なお, 意見の投稿に伴う, 住所, 氏名, 所属などの個人情報については, 学会のプライバシーポリシーに準じて取り扱いたします。 <URL : <https://www.ipsj.or.jp/privacypolicy.html>>

応募先 〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F
一般社団法人 情報処理学会 会誌編集部 E-mail : editj@ipsj.or.jp Fax (03) 3518-8375
<https://www.ipsj.or.jp/magazine/enquete.html>

ご意見をお寄せ
ください!



● 論文誌ジャーナル掲載論文リスト

Vol.62 No.3 (Mar. 2021)

【特集：快適な運用管理を支えるインターネットと運用技術】

- 特集「快適な運用管理を支えるインターネットと運用技術」の編集にあたって 敷田幹文
- クラウドメールサービスのアドレス管理委譲補充方法 嶋吉隆夫 他
- HeteroTSDB: 異種分散 KVS 間の自動階層化による高性能な時系列データベース 坪内佑樹 他
- AXARPSC: Scalable ARP Snooping Using Policy-Based Mirroring of Core Switches with ARP Log Contraction Motoyuki Ohmori 他
- 辞書に基づく DGA マルウェアに起因した悪性ドメインの判別 佐藤彰洋 他
- アプリケーション識別機能付きファイアウォールのログを対象とした機械学習による自己らしい通信の識別手法 市之瀬樹生 他

【特集：若手研究者】

- 特集「若手研究者」の編集にあたって 湊 真一
- oTree を用いた配属システムの設計・構築とその運用 島田夏美 他
- 自己組織型パーティクルフィルタを用いた NIRS による認知負荷強度推定 藤原敏輝 他
- futaba: スマートビルのためのビッグデータ・プラットフォーム 粕谷貴司 他
- ミドルウェアに対する Coverage-based Greybox Fuzzing の適用 伊藤弘将 他
- 不均衡分類問題としての小説の段落境界推定 飯倉 陸 他
- 単言語話者のための日英コードスイッチング音声の認識と翻訳 中山佐保子 他
- Construction of a Switching Support System for Live Broadcast of Oral Presentation Shiori Endo 他

【特集：組込みシステム工学】

- 特集「組込みシステム工学」の編集にあたって 中條拓伯
- Accurate Contention-aware Scheduling Method on Clustered Many-core Platform Shingo Igarashi 他
- CoSAM: Co-Simulation Framework for ROS-based Self-driving Systems and MATLAB/Simulink Keita Miura 他
- ROS ノード軽量実行環境 mROS のユーザ定義メッセージ型の対応のための機能拡張 祐源英俊 他
- Generating Adversarial Examples for Hardware-Trojan Detection at Gate-Level Netlists Kohei Nozawa 他

【一般論文】

- 円周上の max-min 5-dispersion 問題 角田倫久 他
- A Self-Stabilizing 1-maximal Independent Set Algorithm* Hideyuki Tanaka 他
- 多観点類似度を用いた凝集型階層クラスタリング 藤原勇二 他
- Novel Bi-Directional Flow-based Traffic Generation Framework for IDS Evaluation and Exploratory Data Analysis Korakoch Wilailux 他
- 分散アンテナ型アクセスポイントによる無線 LAN 端末 2 次元位置推定* 細田真道 他
- New Proof Techniques Using the Properties of Circulant Matrices for XOR-Based (k; n) Threshold Secret Sharing Schemes † Koji Shima 他
- 株価の日次・月次推移と学習期間調整 吉田健一
- Replay attack detection based on spatial and spectral features of stereo signal Ryoya Yaguchi 他
- 知覚刺激を提示するウェアラブルデバイスがユーザの主観時間に与える影響 清水友順 他

*: 推薦論文 Recommended Paper

†: テクニカルノート Technical Note



● 論文誌トランザクション掲載論文リスト

(Mar. 2021)

【論文誌 コンシューマ・デバイス&システム Vol.11 No.1】

- ネットワーク接続された組込みシステムの拡張 寺岡秀敏 他
- DIY-SDFS: オンサイト利用を想定した IoT データ向け複数 NAS 統合型ファイルシステム 岡本祐樹 他
- 「第二水面」形成による沖合養殖のための水中給餌方式の提案 今井哲郎 他



【論文誌 数理モデル化と応用 Vol.14 No.2】

- Multi-Agent Reinforcement Learning Based Approach for Periodic-Review Joint Replenishment Problem under Practical Cost Structures Hiroshi Suetsugu 他
- 仮想風景における VR 酔い低減のための一手法 笹山琴由 他



◎ IPSJ カレンダー◎

学会イベントの最新情報を下記 URL でご案内しています。新型コロナウイルス感染症拡大を受け、開催方法の変更、開催中止などの可能性がありますので、最新情報をご確認いただきますようお願いいたします。

<https://www.ipsj.or.jp/calendar.html>



【重要】過去のプログラミング・シンポジウム報告集の利用許諾について

2020年12月18日

プログラミング・シンポジウム委員会

情報処理学会発行の出版物著作権は平成12年から情報処理学会著作権規程に従い、学会に帰属することになっています。

プログラミング・シンポジウムの報告集は、情報処理学会と設立の事情が異なるため、この改訂がシンポジウム内部で徹底しておらず、情報処理学会の他の出版物が情報学広場 (= 情報処理学会電子図書館) で公開されているにもかかわらず、古い報告集には公開されていないものが少からずありました。

プログラミング・シンポジウムは昭和59年に情報処理学会の一部門になりましたが、それ以前の報告集も含め、このたび学会の他の出版物と同様の扱いにしたいと考えます。過去のすべての報告集の論文について、著作権者（論文を執筆された故人の相続人）を探し出して利用許諾に関する同意をいただくことは困難ですので、一定期間の権利者搜索の努力をしたうえで、著作権者が見つからない場合も論文を情報学広場に掲載させていただきたいと思っております。その後、著作権者が発見され、情報学広場への掲載の継続に同意が得られなかった場合には、当該論文については、掲載を停止いたします。

この措置にご意見のある方は、プログラミング・シンポジウムの辻尚史運営委員長 (tsuji@math.s.chiba-u.ac.jp) までお申し出ください。

加えて、著作権者について情報をお持ちの方は事務局まで情報をお寄せくださいますようお願い申し上げます。

期間：2020年12月18日～2021年3月19日

情報処理学会著作権規程

<https://www.ipsj.or.jp/copyright/ronbun/copyright.html>

IPSJ メールニュースへ広告を出しませんか？

広告をIPSJメールニュースで配信しています。本会会員が主な読者なので、ターゲットを絞った広告に最適です。

- 配 信 数：約32,000通（原則毎週月曜日配信）
- 読 者 層：本会会員および非会員
- 形 式：テキストのみ。等幅半角70字×5行。URLを入れてください。
- 掲載位置：ヘッダ（目次の上）
フッタ（本文の最下行）
- 掲 載 料：ヘッダ：1回50,000円（税抜）※3社限定
フッタ：1回20,000円（税抜）
※それぞれ行数超過については別途相談
- 申 込 先：[広告代理店]
アドコム・メディア（株）E-mail: sales@adcom-media.co.jp
〒169-0073 東京都新宿区百人町2-21-27 Tel(03)3367-0571 Fax(03)3368-1519
または、情報処理学会 会誌編集部 E-mail: editj@ipsj.or.jp Tel(03)3518-8371
- 申込締切：毎週水曜日締切、翌週月曜日配信となります。
- 見 本：

— [広告] —

■■■■ ○○セミナー ■■■■

開催日時：1月10日（火）・11日（水）・12日（木）13：00～17：00

会場：○○コンベンションセンター

会費：情報処理学会会員の方には割引があります。

詳細はこちらをご覧ください：<http://www.....com/>

— [広告] —

【ご案内】会誌「情報処理」のオンライン記事について

会誌「情報処理」の特集記事は、これまで冊子、オンライン（電子図書館）の両方に掲載しておりましたが、次のとおり オンラインのみへの掲載 に変わりました。また、オンライン限定記事の掲載も始まりました。

◆開始月：2020年11月号（発行日：2020年10月15日）

◆閲覧方法：会員区分によって異なりますので以下をご確認ください。

【個人会員の皆様】

電子図書館（情報学広場：<https://ipsj.ixsq.nii.ac.jp/ej/>）にログインし、該当記事のpdfをダウンロードしてください。すでに電子図書館をご利用いただいている方は今までどおりです。

電子図書館を初めて利用される方は、会員としてのユーザ登録が必要になります。

未登録の方には毎月上旬に次の件名のメールを送信しておりますので、到着次第、登録してください。

- 件名：[情報学広場:情報処理学会電子図書館] ユーザー登録のご案内
- 差出：ipsj-ixsq@nii.ac.jp

【個人会員】



電子図書館
(情報学広場)

★詳細：電子図書館利用方法（個人用）－利用までの流れ（<https://www.ipsj.or.jp/e-library/ixsq.html#anc2>）

ご案内メールをお急ぎの方や閲覧方法が分からない方は、会員サービス部門（E-mail: mem@ipsj.or.jp）に会員番号を添えてご連絡ください。

【賛助会員各位・購読員の皆様】

賛助会員・購読員の企業・大学に所属されている方に「情報処理」（冊子）を貸し出した場合、特集の閲覧方法について照会がございましたら、次の手順をお知らせください。

<手順>

- (1) 「情報処理」の特集ページ（扉または概要ページ）を開く。
- (2) 閲覧申込のURLにアクセスする（またはQRコードを読み取る）。
- (3) 必須事項を入力し送信する。
- (4) 次の件名（4月号の場合）の受信メールに従って、電子図書館から特集のpdfをダウンロードする。
 - 件名：情報処理 2021年4月号（Vol.62, No.4）「チケットコード」とご利用方法のご連絡

★注意事項

- 法人アカウントではご利用いただけません。
- 閲覧される方が電子図書館のユーザIDをお持ちでない場合は、ご自身でユーザ登録する必要があります。

本件に関する問合せ先：一般社団法人情報処理学会 会員サービス部門 E-mail: mem@ipsj.or.jp



人材募集 (有料会告)

申込方法: 任意の用紙に件名, 申込者氏名, 勤務先, 職名, 住所, 電話番号および請求書に記載する「宛名」, Web掲載の有無などを記載し, 掲載希望原稿 ([募集職種, 募集人員, (所属), 専門分野, (担当科目), 応募資格, 着任時期, 提出書類, 応募締切, 送付先, 照会先]) を添えて下記の申込先へ, E-mail, Fax または郵送にてお申し込みください。

*都合により編集させていただく場合がありますので, ご了承ください。

申込期限: 毎月15日を締切日とし翌月号(15日発行)に掲載します。

掲載料金: 国公立教育機関, 国公立研究機関 税抜 20,000円 (税込 22,000円)

賛助会員 (企業) 税抜 30,000円 (税込 33,000円)

賛助会員以外の企業 税抜 50,000円 (税込 55,000円)

*本誌へ掲載依頼いただいた場合に限り, 追加料金 税抜 4,000円 (税込 4,400円) で同一内容を本誌 Web ページに掲載できます。

申込先: 情報処理学会 会誌編集部 (有料会告係) E-mail: editj@ipsj.or.jp Fax(03)3518-8375

*原稿受付の際には必ず原稿受領のお知らせを差し上げています。もし3日以内(土日祝日除く)に返信がない場合は念のため確認のご連絡をください。

*特に指定がないかぎり履歴書には写真を貼付のこと

■国立研究開発法人情報通信研究機構

国立研究開発法人情報通信研究機構 (NICT) は, 情報通信分野を専門とする我が国唯一の公的研究機関として, 情報通信に関する技術の研究開発を基礎から応用まで統合的な視点で推進し, 同時に, 大学, 産業界, 自治体, 国内外の研究機関などと連携し, 研究開発成果を広く社会へ還元し, イノベーションを創出することを目指しています。当機構では, 情報通信技術の研究開発推進のため, 優秀で意欲のある研究者を広く公募いたします。

募集職種 パーマネント研究職員, パーマネント研究技術職員およびテニュアトラック研究員

採用時期 2022年4月1日 (場合により早期採用の可能性あり)

応募方法 当機構採用情報の Web ページからのエントリー (研究職)

https://www.nict.go.jp/employment/research_staff.html

(研究技術職)

https://www.nict.go.jp/employment/technical_staff.html

応募締切 2021年4月9日 (17:00 必着)

照会先 〒184-8795 東京都小金井市貫井北町 4-2-1

国立研究開発法人情報通信研究機構 総務部人事室人事グループ
/経営企画部 研究職採用担当 E-mail: jinji-r@m1.nict.go.jp

Tel(042)327-7304 Fax(042)327-7590

その他 詳細は当機構採用情報の Web ページにてご確認ください

■東京都市大学メディア情報学部情報システム学科

募集人員 ①教授 ②准教授 ③講師 (任期付) ④講師 (テニュアトラック) いずれか1名

専門分野 経営情報システム, ICT アセスメント, ICT マネジメント, IT サービス, 組織管理

着任時期 2021年9月1日

応募締切 2021年4月16日 (当日消印有効)

その他 【詳細】東京都市大学採用情報 メディア情報学部情報システム学科 <https://www.tcu.ac.jp/recruitinformation/>





FIT2021 第20回情報科学技術フォーラム

選奨論文・一般論文 講演募集予告

会 期：2021年8月25日（水）～27日（金）

会 場：東北学院大学（オンライン）

FIT2021 Web ページ <https://www.ipsj.or.jp/event/fit/fit2021/>

受付期間(予定)：2021年3月29日（月）～5月7日（金）

◆論文ページ数：2～8ページ程度 ◆講演時間：20分

◆3ページ目以降は追加ページ代（4,000円/ページ）が必要です

電子情報通信学会 情報・システムソサイエティ (ISS) 並びにヒューマンコミュニケーショングループ (HCG) と情報処理学会 (IPSJ) は、2002年から毎年秋季に合同で「情報科学技術フォーラム(FIT: Forum on Information Technology)」を開催しています。2021年8月には、記念すべき第20回目を東北学院大学（オンライン）で開催します。FITは、両学会の大会の流れをくむものであると同時に、従来の大会の形式にとらわれずに新しい発表形式を導入し、タイムリーな情報発信、活気ある議論・討論、多彩な企画、他分野研究者との交流を実現してきております。皆様の研究成果発表の場として、標記のとおり論文発表を募集致しますので奮ってお申込み下さい。

●申込主要日程（予定）

登録申込/投稿受付期間：2021年3月29日（月）から 2021年5月7日（金）まで

最終掲載原稿締切：2021年6月18日（金）

※ FIT2017 より、査読付き論文は廃止とし、選奨論文制度を取り入れました。

※ 登録申込と原稿投稿は上記のFIT2021 Webページよりお願い致します。詳細は決定次第 Webページでお知らせ致します。

●表彰

FITには、以下の表彰制度がありますので是非ともチャレンジして下さい。

いずれの賞も、電子情報通信学会又は情報処理学会の会員であることが受賞条件となりますのでこの機会に是非御入会下さい。

船井ベストペーパー賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上3件選定。賞金は船井情報科学振興財団より20万円贈呈。
FIT 論文賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上7件程度選定。賞金はFIT 運営委員会より5万円贈呈。
FIT ヤングリサーチアワード賞	2021年12月31日現在で33歳未満の講演者（選奨論文および一般論文）の中から、発表件数の1.5%を上限として選定。賞金はFIT 運営委員会より3万円贈呈。本賞受賞は本人に対し一回のみ。
FIT 奨励賞	一般発表のセッション毎に座長の裁量で優秀な発表を1件その場で選定（該当なしもあり）。FIT 終了後に賞状を贈呈。

●選奨論文（4～8 ページ程度）

投稿された論文の担当研究会を決定していただきます。FIT2021 Web ページに掲載の研究会取り扱い分野をよく御確認のうえ御自身の論文内容と一致した研究会を、申込者御自身の責任において投稿時に適切に選択して下さい。

船井ベストペーパー賞、FIT 論文賞への審査を希望する場合は、Web からの講演申込みの際に必ず論文形式で『選奨論文』を選択して下さい。但し、賞を前提とした論文形式となりますので、電子情報通信学会又は情報処理学会の会員であることが投稿条件となります。非会員の方は御入会手続きをお済ませの上御投稿下さい。選奨論文はFIT 初日の選奨セッションに組み込まれ、各セッションにて選奨委員2名による1次審査を行います。1次審査の結果は当日の夕方までに大会会場に掲示されます。2次審査はFIT 終了後実施され、上位3件が船井ベストペーパー賞、次点7件程度が FIT 論文賞の受賞となります。

※4 ページ以上の投稿が必須ですが、3 ページ目からは追加ページ代（4,000円/ページ）が発生します。例えば6 ページ投稿の場合、4 ページ分の追加ページ代が発生しますので、講演参加費のほかに「4,000円×4=16,000円」の追加費用が必要となります。

●一般論文（2～8 ページ程度）

FIT2021 Web ページに掲載の研究会取り扱い分野をよく御確認のうえ御自身の論文内容と一致した研究会を、申込者御自身の責任において適切に選択して下さい。

※3 ページ以上の投稿される場合は、3 ページ目からは追加ページ代（4,000円/ページ）が発生します。例えば4 ページ投稿の場合、2 ページ分の追加ページ代が発生しますので、講演参加費のほかに「4,000円×2=8,000円」の追加費用が必要となります。

●論文誌推薦制度

選奨論文の中から船井ベストペーパー賞の審査を通して優秀な論文と判断されたものを、FIT プログラム委員会が電子情報通信学会または情報処理学会 (FIT 講演申込フォームの講演応募分野 (研究会) で選択した研究会が属する学会) の論文誌へ推薦します。掲載の採否は、それぞれの学会の論文誌編集委員会が決定します。論文誌への投稿の際には、投稿先論文誌編集委員会の評価基準を満足しうる、完成度の高い論文に仕上げてください。なお、推薦を辞退することも可能です。

●問合せ先（FIT2021事務局）

〒101-0062 千代田区神田駿河台1-5 化学会館4階

情報処理学会 事業部門 TEL. 03-3518-8373 FAX. 03-3518-8375 E-mail: ipsjfit@ipsj.or.jp

◆◆ 有料会告について ◆◆

本会の主催・共催行事および協賛・後援記事の次第書（論文募集，参加案内等）の本誌掲載については，下記により有料にて取り扱っていますのでお知らせします。

記

■掲載条件

件名	内容	掲載単位	掲載料金（税抜）	
論文募集／ 参加者募集	国際会議，シンポジウム，ワークショップ，講演会，講習会などの論文募集・参加者募集	1 ページ，1/2 ページ または 1/4 ページ	(主催・共催)	
			1 ページ	50,000 円
			1/2 ページ	30,000 円
			1/4 ページ	20,000 円
			(協賛)	
広告として取り扱う				
人材募集	国公立教育機関，国公立研究機関， 企業の人材募集	10 行程度	国公立教育機関，国公立研究機関	20,000 円
			賛助会員（企業）	30,000 円
			賛助会員以外の企業	50,000 円
* 本会誌へ掲載依頼いただいた場合に限り，追加料金 4,000 円で同一内容を本会 Web ページに掲載できます。				

■申込方法 任意の用紙に，件名，申込者氏名，勤務先，職名，住所，電話番号および請求書宛先，Web 掲載の有無（人材募集のみ）などを記載し，掲載希望原稿を添えて下記の申込先へお申し込みください。

■原稿の書き方

- 行事次第書： A4 変形判カメラレディまたは PDF ファイル（フォント埋め込み）とします。
(1 ページ) 天地 250mm × 左右 180mm
(1/2 ページ) 天地 120mm × 左右 180mm
(1/4 ページ) 天地 55mm × 左右 180mm
* A4 変形判以外の原稿は縮小または拡大となりますのでご注意ください。
- 人材募集： 次の項目を明記し，E-mail または Fax，郵送にてお送りください。
[募集職種，募集人員，(所属)，専門分野，(担当科目)，応募資格，着任時期，提出書類，応募締切，送付先，照会先]
* なお，都合により編集させていただく場合がありますので，ご了承ください。

■申込期限 毎月 15 日を締切日とし，翌月号（15 日発行）に掲載します。

■掲載料金 掲載号発行日に料金を請求いたしますので，3 カ月以内にお支払いください。

■掲載申込先 一般社団法人 情報処理学会 会誌編集部門（有料会告係）
〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F
E-mail: editj@ipsj.or.jp Tel (03) 3518-8371 Fax (03) 3518-8375

「情報処理」 カタログ同封サービスの ご案内

？
 カタログ同封
 サービスとは？

毎月会員に配布している学会誌に貴社/貴校のカタログや広告を同封し、直接読者にお届けするサービスです。
 通常のDMと異なり学会誌に同封しますので、**読者の開封率は格段に上がります**。
 また、カタログ送付にかかる**コストを最小に抑えることができ**、なおかつ情報処理を専門とする読者に**ターゲットを絞った効果的な案内を出すことが可能**となります。



- ### お申し込み方法と掲載までの手続き
- 封入希望月の前月15日までに下記事項を記載の上、問合せ先までお申し込みください。
 - ◆会社名、担当者、連絡先（住所、Tel、Fax、E-mail） ◆封入希望号
 - ◆サイズ ◆カタログの簡単な内容説明
 - ◆割引対象にあたる場合はその旨記載ください。
 - 封入希望月の遅くとも前月末日までに下記事項について手配をお願いします。
 - ◆カタログ見本を問合せ先までお送りください（PDF、Fax可）。
 - ◆納品業者をお知らせください。
 - 納品日は封入希望月の5日（土曜、日曜、祝日の場合は翌営業日）です。日付指定にて必要枚数（20,000枚）を印刷し指定の納品先へお送りください。
 - ※納品先は、お申し込み後にご連絡いたします。
 - ※納品が遅れますと同封ができない場合がございます。その場合はキャンセルとさせていただきます。
 - カタログを同封した学会誌を発行日にお送りしますので、ご確認ください。
 - 後日請求書をお送りしますので振込手続きをお願いします。

1通あたり
 約17.5円！ **基本価格 350,000円**
 (税抜)

対象：全会員 20,000通 配布
 (正会員 / 名誉会員 / 学生会員 / 賛助会員)

大学や
 共催事業は
 さらに割引も！

大学 / 研究所 / 賛助会員または情報処理学会主催・共催事業は、下記のとおり割引料金が適用されます。

大学 / 研究所 / 賛助会員
 (基本価格の40% Off!) **210,000円**
 (税抜)

情報処理学会主催・共催事業*
 (基本価格の80% Off!) **70,000円**
 (税抜)

*情報処理学会研究会主催、共催を含む

サイズ：A4変形判またはA4判二つ折り（その他についてはご相談ください）
 用紙：色上質厚口（四六判80kg）またはコート紙（四六判90kg）相当

問合せ先
 [広告代理店] アドコム・メディア(株) E-mail: sales@adcom-media.co.jp
 〒169-0073 東京都新宿区百人町2-21-27
 Tel.(03)3367-0571 Fax.(03)3368-1519

一般社団法人情報処理学会 会誌編集部 E-mail: editj@ipsj.or.jp
 〒101-0062 東京都千代田区神田駿河台1-5 化学会館4F
 Tel.(03)3518-8371 Fax.(03)3518-8375



大学・工業高校・専門学校などで
教科書・参考書としてお使いいただけるシリーズです。

新刊

一般情報教育 (一般教育シリーズ)

稲垣知宏・上繁義史・北上 始・佐々木整・高橋尚子・
中鉢直宏・徳野淳子・中西通雄・堀江郁美・水野一徳・
山際 基・山下和之・湯瀬裕昭・和田 勉・渡邊真也 著
A5判/266頁/本体2,200円(税別)

オペレーティングシステム (改訂2版)

野口健一郎・光来健一・品川高廣 共著
A5判/256頁/本体2,800円(税別)

ネットワークセキュリティ

菊池浩明・上原哲太郎 共著
A5判/206頁/本体2,800円(税別)

ソフトウェア工学

平山雅之・鶴林尚靖 共著
A5判/214頁/本体2,600円(税別)

応用Web技術 (改訂2版)

松下 温 監修/市村 哲・宇田隆哉 共著
A5判/192頁/本体2,500円(税別)

基礎Web技術 (改訂2版)

松下 温 監修/市村 哲・宇田隆哉・伊藤雅仁 共著
A5判/196頁/本体2,500円(税別)

画像工学

堀越 力・森本 正志・三浦康之・澤野弘明 共著
A5判/232頁/本体2,800円(税別)

人工知能 (改訂2版)

本位田真一 監修/松本一教・宮原哲浩・
永井保夫・市瀬龍太郎 共著
A5判/244頁/本体2,800円(税別)

音声認識システム (改訂2版)

河原達也 編著
A5判/208頁/本体3,500円(税別)

ヒューマンコンピュータ
インタラクション (改訂2版)

岡田謙一・西田正吾・葛岡英明・仲谷美江・塩澤秀和
共著 A5判/260頁/本体2,800円(税別)

ソフトウェア開発 (改訂2版)

小泉寿男・辻 秀一・吉田幸二・中島 毅 共著
A5判/224頁/本体2,800円(税別)

情報と職業 (改訂2版)

駒谷昇一・辰己丈夫 共著
A5判/232頁/本体2,500円(税別)

情報通信ネットワーク

阪田史郎・井関文一・小高知宏・甲藤二郎・
菊池浩明・塩田茂雄・長 敬三 共著
A5判/288頁/本体2,800円(税別)

数理最適化

久野善人・繁野麻衣子・後藤順哉 共著
A5判/272頁/本体3,300円(税別)

情報とネットワーク社会 (一般教育シリーズ)

駒谷昇一・山川 修・中西通雄・北上 始・佐々木整・
湯瀬裕昭 共著 A5判/196頁/本体2,200円(税別)

情報とコンピュータ (一般教育シリーズ)

河村一樹・和田 勉・山下和之・立田ルミ・岡田 正・
佐々木整・山口和紀 共著
A5判/176頁/本体2,200円(税別)

メディア学概論

山口治男 著
A5判/172頁/本体2,400円(税別)

情報ネットワーク (一般教育シリーズ)

岡田 正・駒谷昇一・西原清一・水野一徳 共著
A5判/168頁/本体2,300円(税別)

離散数学

松原良太・大高彰昇・藤田慎也・小関健太・
中上川友樹・佐久間雅・津垣正男 共著
A5判/256頁/本体2,800円(税別)

HPCプログラミング

寒川 光・藤野清次・長嶋利夫・高橋大介 共著
A5判/256頁/本体2,800円(税別)

ユビキタスコンピューティング

松下 温・佐藤明雄・重野 寛・屋代智之 共著
A5判/232頁/本体2,800円(税別)

Java/UMLによる
アプリケーション開発

森澤好臣 監修/布広永示・高橋英男 共著
A5判/208頁/本体2,600円(税別)

情報理論

白木善尚 編
村松 純・岩田賢一・有村光晴・波谷智治 共著
A5判/256頁/本体2,800円(税別)

Java基本プログラミング

今城哲二 編 布広永示・
マッキンケネスジェームス・大見嘉弘 共著
A5判/248頁/本体2,500円(税別)

システムLSI設計工学

藤田昌宏 編著
A5判/242頁/本体2,800円(税別)

組込みシステム

阪田史郎 著 高田広章 編著
A5判/280頁/本体3,000円(税別)

情報システム基礎 (一般教育シリーズ)

神沼靖子 編著
A5判/228頁/本体2,500円(税別)

Linux演習

前野譲二・落合 昭・生野荘一郎・塩澤秀和・
高島俊徳 共著
A5判/224頁/本体2,500円(税別)

インターネットプロトコル

阪田史郎 編著
A5判/272頁/本体2,800円(税別)

分散処理

谷口秀夫 編著
A5判/240頁/本体2,800円(税別)

情報とコンピューティング
(一般教育シリーズ)

川合 慧 監修/河村一樹 編著
A5判/228頁/本体2,500円(税別)

情報と社会 (一般教育シリーズ)

川合 慧 監修/駒谷昇一 編著
A5判/236頁/本体2,500円(税別)

コンピュータアーキテクチャ (改訂2版)

小柳 滋・内田啓一郎 共著
A5判/256頁/本体2,900円(税別)

コンピュータグラフィックス

魏 大名・先田和弘・Roman Durikovic・向井信彦・
Carl Vilbrandt 共著
A5判/280頁/本体3,000円(税別)

アルゴリズム論

浅野哲夫・和田幸一・増澤利光 共著
A5判/242頁/本体2,800円(税別)

データベース

速水治夫・宮崎収一・山崎晴明 共著
A5判/196頁/本体2,500円(税別)

ソフトウェア工学演習

伊藤 潔・廣田豊彦・富士 隆・熊谷 敏・川端 亮 共著
A5判/228頁/本体2,800円(税別)

データベースの基礎

吉川正俊 著
A5判/288頁/本体2,900円(税別)

コンピュータグラフィックスの基礎

宮崎大輔・床井浩平・結城 修・吉田 典正 著
A5判/292頁/本体3,200円(税別)

本体価格(税別)は変更する場合があります。

注文はオーム社Webサイトまで ▶ https://www.ohmsha.co.jp/tbc/text_series_0202.htm

ご寄付のお願い

情報処理学会は、情報処理に関する学術および技術の振興をはかることにより、学術、文化ならびに産業の発展に寄与することを目的に各種事業を戦略的に展開しております。今回、学会活動の更なる活性化を図る上で会員の皆様からご寄付を頂戴いたしたく、お願いを申し上げます。

皆様から頂きますご寄付は

情報技術を通じて、人類及び世界の発展に資するため
情報技術を中心に学術および技術の振興に資するため
将来を担う人材の育成に資するため

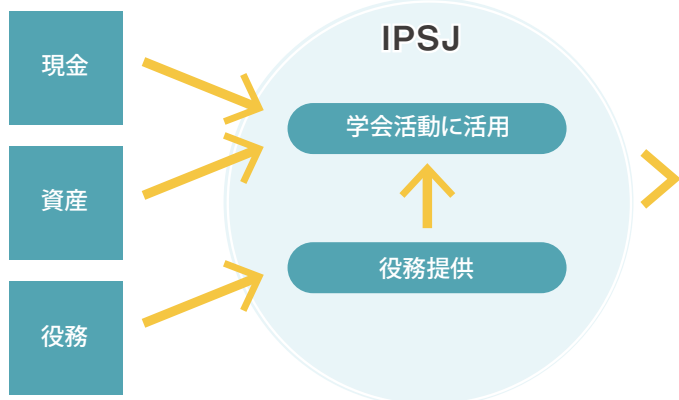
などの観点に照らし、下記の項目に活用させて頂く所存です。

今回ご寄付をお願いしたいのは現金に加えて、情報技術に関わる有形無形の資産（著作物、電子コンテンツ、特許、ソフトウェア等）、ボランティアで提供いただける役務提供（経験や知識に基づく役務）なども含まれます。お預かりいたしましたご寄付のうち用途のご指定のあるものは、そのご意向に沿った活用をさせて頂き、ご指定のないものは、その用途を学会活動の活性化に有効な諸事業で活用させて頂きます。今後も会員の皆様の絶大なるご支援・ご協力を頂きながら、学会発展のために努力して参る所存でありますので、何卒よろしくごお願い申し上げます。

* ご注意 情報処理学会は寄付金に対する税金が優遇される特定公益増進法人ではございません。

IPSJ 寄付

会員他寄付



活用先

教育・育成

情報入試 | 子ども教室 | パソコン教室

社会貢献

表彰

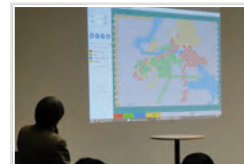
国際活動

規格標準化

情報資産保存

学会諸事業

その他



詳しくはこちら

<https://www.ipsj.or.jp/annai/other/donation.html>

お問合せ

一般社団法人 情報処理学会 管理部門

〒101-0062 東京都千代田区神田駿河台1-5 化学会館4F

TEL 03-3518-8374 FAX 03-3518-8375

✉ soumu@ipsj.or.jp

CONTENTS

Preface

- 184 What Can We Do for "No One Left Behind"?
Chieko ASAKAWA (IBM)

Special Features

Engrossed in Quantum Technology

- 186 Foreword
Mikiko SODE TANAKA (International College of
Technology)
188 Outline

"Peta-gogy" for Future

- 191 Issues of ICT in Education
Kentaro MAEDA (Hokkaido Sapporo Kita Senior
High School)

Let's Learn Informatics

- 192 Entrance Exam Analysis with Text Mining
Takashi NAKAYAMA (Tokyo Metropolitan Meguro
High School)

- 199 Questions for Experts
200 Biblio Talk
202 Skimming a Famous Paper in Five Minutes
204 Conference Report

Online Only

Special Features

Engrossed in Quantum Technology

- e1 Daybreak of Quantum Computers
Hiroshi IMAI (The Univ. of Tokyo)
e8 Quantum Annealing is Dead?
Masayuki OHZEKI (Tohoku Univ.)
e15 Utilization of Next Generation Accelerators Using
Quantum Technology
Masashi TAWADA (Waseda Univ.), Shu TANAKA
(Keio Univ.), Yoshiki MATSUDA (Fixstars Corp.) and
Tenin YAN (QunaSys Inc.)
e22 Quantum Computation for Finance
Shumpei UNO (Mizuho Information & Research
Institute, Inc.)
e28 Quantum Computer and Quantum Chemistry
- Does Quantum Computer Bring Benefit to
Quantum Chemistry? -
Yu-ya OHNISHI (JSR Corp.)

- e35 Quantum Computing for Machine Learning
- Near-term and Long-term Algorithms -
Kosuke MITARAI (Osaka Univ.)
e41 Potential of Diamond
- Solid-state Quantum Sensors -
Mutsuko HATANO (Tokyo Institute of Technology)
e47 The Principle of Quantum Cryptography and
Developments for Its Practical Realization
Akihiro MIZUTANI (Mitsubishi Electric Corp.,
Information Technology R&D Center)
e53 Quantum Virtual Hackathon - Raising Quantum
Talents by the Community
Yuri KOBAYASHI, Atsushi MATSUO and Kifumi
NUMATA (IBM Research - Tokyo)

Article

- e61 Commentary on "Design Guideline for
Information Education Courses"
Masami HAGIYA (The Univ. of Tokyo)

読後のご意見をお送りください

本誌では、現在約 200 名の方々に毎号のモニタをお願いしておりますが、より多くの読者の皆さんからのご意見、ご提案をおうかがいし、誌面の充実に役立てていきたいと考えておりますので、以下 Web ページから奮って事務局までお寄せください。

「情報処理」アンケートページ <https://www.ipsj.or.jp/magazine/enquete.html>

一般社団法人 情報処理学会 会誌編集部

〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F E-mail: editj@ipsj.or.jp Fax(03)3518-8371



アンケートページ
QR コード

本会は、本会出版委員会監修でオーム社より『量子コンピューティング—基本アルゴリズムから量子機械学習まで—』を発行している。初めて量子コンピューティングを学ぶ人から研究者まで幅広い方に読んでいただける良書である。また、2021年3月に開催される本会第83回全国大会ではイベント企画として「量子技術を利用した次世代アクセラレータの活用」を企画した。加えて、量子ソフトウェア研究会を運営するなど量子技術に積極的に取り組んでいる。本号の「面白いぞ量子技術」特集は本会での取り組みの一端を知っていただくことを目的としている。私にとってコンピュータは人生の友と言える。スーパーコンピュータであるNEC ACOSシリーズ、SXシリーズの開発に携わり、一緒に成長をさせていただいた。量子コンピュータの時代になり、新しい友に巡り合えた気分で心をワクワクさせられている。スーパーコンピュータの開発は、同時に

その利用方法についても開拓、開発が行われた。量子コンピュータはまだまだよちよち歩きであるが、これから大きく成長し、各種分野での活用が検討され、活用されていくことになると思う。やはりワクワクせずにはいられない。量子技術は、量子コンピュータだけではなく、本特集で解説いただいた量子センサや量子暗号など幅が広い。また、量子技術イノベーション戦略が検討されるなど、日本として国をあげて総合的かつ戦略的な取り組みを展開していくことが決められた重要技術である。今回特集を私が担当するにあたり、量子技術全般をカバーできるように検討を行ったが幅が広すぎて1回の特集ですべてをカバーすることはできなかった。今後今回カバーできなかった技術についても特集を組んで紹介できるように検討したい。

(袖美樹子/本特集エディタ)

次号(5月号) 予定目次

編集の都合により変更になる場合がありますのでご了承ください。

※はオンライン版のみの掲載となります

「特集」より自由でより没入感の高いイマージブメディアに向けた研究開発*

自由視点テレビFTVの原理/超高臨場ライブ体験の開発と標準化/イマージブメディアに向けた音響技術—放送とMPEGを中心に—/MPEGが規格化に取り組む映像システム技術—新たな映像体験に向けて—

「デジタルプラクティスコーナー」オープンサイエンスを支える研究データ基盤*

[解説論文] オープンサイエンスと研究データ管理の動向/ [解説論文] 統合データベースプロジェクトから学ぶこと

「デジタルプラクティスコーナー」感性情報学 最前線*

感情認識AI「心sensor」の教育現場導入に向けた実証実験/ [解説論文] ユーザの感性情報を用いた動的なコンピュータシステム/遠隔地間の味コミュニケーションを想定した対話型進化計算による混合飲料生成システムの改善/対話型進化計算システムにおける一対比較評価の有用性/インタビュー・座談会: 最前線に立つ実務家と研究者が見る感性情報学の今と未来

特別解説: オンライン教育と著作権法第35条運用指針..... 芳賀高洋

解説: 日本語プログラミング言語「なでしこ」に関する解説*..... くじら飛行機

教育コーナー: べた語義

連載: 5分で分かる! ?有名論文ナメ読み/ <Info-WorkPlace 委員会企画> 働き方を共有しよう! * / 買い物自慢/ 情報の授業をしよう/ 先生、質問です! / ビブリオ・トーク

コラム: 巻頭コラム

会議レポート: CCS 2020 会議報告

複写される方へ

一般社団法人情報処理学会では複写複製および転載複製に係る著作権を学術著作権協会に委託しています。当該利用をご希望の方は、学術著作権協会 (<https://www.jaacc.org/>) が提供している複製利用許諾システムもしくは転載許諾システムを通じて申請ください。

尚、本会会員(賛助会員含む)および著者が転載利用の申請をされる場合には、学術目的利用に限り、無償で転載利用いただくことが可能です。ただし、利用の際には予め申請いただくようお願い致します。

権利委託先: 一般社団法人学術著作権協会
〒107-0052 東京都港区赤坂9-6-41 乃木坂ビル
E-mail: info@jaacc.jp Tel (03)3475-5618 Fax (03)3475-5619

また、アメリカ合衆国において本書を複写したい場合は、次の団体に連絡してください。
Copyright Clearance Center, Inc.
222 Rosewood Drive, Danvers, MA 01923 USA
Phone: 1-978-750-8400 Fax: 1-978-646-8600

Notice for Photocopying

Information Processing Society of Japan authorized Japan Academic Association For Copyright Clearance (JACC) to license our reproduction rights and reuse rights of copyrighted works. If you wish to obtain permissions of these rights in the countries or regions outside Japan, please refer to the homepage of JACC (<http://www.jaacc.org/en/>) and confirm appropriate organizations.

You may reuse a content for non-commercial use for free, however please contact us directly to obtain the permission for the reuse content in advance.

<All users except those in USA>

Japan Academic Association for Copyright Clearance, Inc. (JAACC)
6-41 Akasaka 9-chome, Minato-ku, Tokyo 107-0052 Japan
E-mail: info@jaacc.jp
Phone: 81-3-3475-5618 Fax: 81-3-3475-5619

<Users in USA>

Copyright Clearance Center, Inc.
222 Rosewood Drive, Danvers, MA 01923 USA
Phone: 1-978-750-8400 Fax: 1-978-646-8600

広告のお申込み

■広告料金表

掲載場所	4色	1色
表2	330,000円 (税抜)	—
表3	275,000円 (税抜)	—
表4	385,000円 (税抜)	—
表2対向	300,000円 (税抜)	—
表3対向	265,000円 (税抜)	155,000円 (税抜)
前付1頁	250,000円 (税抜)	135,000円 (税抜)
前付1/2頁	—	80,000円 (税抜)
前付最終	—	148,000円 (税抜)
目次前	—	148,000円 (税抜)
差込 (A4変形判 70.5kg未満 1枚)	275,000円 (税抜)	
差込 (A4変形判 70.5kg～86.5kg 1枚)	350,000円 (税抜)	
同封 (A4変形判 1枚)	350,000円 (税抜)	

■「情報処理」

発行 一般社団法人 情報処理学会
 発行部数 20,000部
 体裁 A4変形判
 発行日 毎月15日
 申込締切 前月10日
 原稿締切 前月20日
 広告原稿 完全版下データ
 原稿寸法 1頁 天地250mm×左右180mm
 1/2頁 天地120mm×左右180mm
 雑誌寸法 天地280mm×左右210mm

■問合せ・お申込み先

〒169-0073 東京都新宿区百人町2-21-27
 アドコム・メディア(株) (Tel/Fax/E-mailは下に記載)

*原稿制作が必要な場合には別途実費申し受けます。
 *同封のサイズ・割引の詳細についてはお問合せください。

掲載広告の資料請求

掲載広告の詳しい資料をご希望の方は、ご希望の会社名にチェック☑を入れ、送付希望先をご記入の上、Faxにて（またはE-mailにて必要事項を記入の上）アドコム・メディア（株）宛にご請求ください。

■「情報処理」 62巻4号 掲載広告（五十音順）

- MCPC..... 表3 とめ研究所..... 目次前上
 キオクシア..... 表4
 電子情報通信学会..... 目次前下 すべての会社を希望

■資料送付先

フリガナ
お名前 _____

勤務先 _____ 所属部署 _____

所在地 (〒 -) _____

TEL () - FAX () -

ご専門の分野 _____



お問合せ・お申込み・資料請求は

広告総代理店 **アドコム・メディア(株)**

Tel.03-3367-0571 Fax.03-3368-1519 E-mail: sales@adcom-media.co.jp

賛助会員のご紹介

本会をご支援いただいております賛助会員をご紹介します。
Web サイト (<https://www.ipsj.or.jp/annai/aboutipsj/sanjo.html>) 「賛助会員一覧」のページからも
各社へリンクサービスを行っておりますので、ぜひご覧ください。

照会先 情報処理学会 会員サービス部門 E-mail: mem@ipsj.or.jp Tel.(03)3518-8370

●●● 賛助会員 (20 ~ 50口)

HITACHI
Inspire the Next

(株) 日立製作所



三菱電機 (株)

FUJITSU

富士通 (株)



(株) サイバーエージェント

Orchestrating a brighter world

NEC

日本電気 (株)



日本アイ・ビー・エム (株)

●●● 賛助会員 (10 ~ 19口)

RECRUIT

(株) リクルート

Google

グーグル合同会社

docomo

(株) NTTドコモ

TOSHIBA

(株) 東芝



日本電信電話 (株)

Microsoft

日本マイクロソフト (株)



(株) フォーラムエイト

●●● 賛助会員 (3 ~ 9口)



(一社) 情報通信技術委員会

NTT Data

(株) NTTデータ

GREE

グリー (株)

Rakuten
Institute of Technology

楽天技術研究所

IA Japan

(一財) インターネット協会



(一社) 情報サービス産業協会



トレンドマイクロ (株)



NTTコムウェア (株)



NTTテクノクロス (株)

uejima

(株) うえじま企画



エッジテクノロジー (株)

OKI

沖電気工業 (株)



キャノンマーケティングジャパン株式会社
キャノンマーケティングジャパン (株)



コアマイクロシステムズ (株)

SANBI

三美印刷 (株)



(株) セプテーニ

SONY

ソニー (株)



チームラボ (株)



(株) テクノプロ
テクノプロ・デザイン社

Panasonic

パナソニック (株)

MIZUHO みずほ情報総研

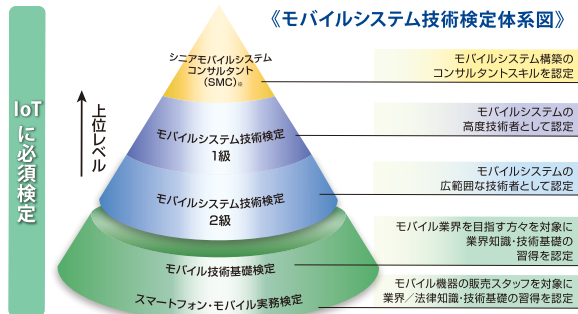
みずほ情報総研 (株)

DX推進の必須資格 5G・IoT・AIエンジニアのための資格試験

2021年度 MCPC 検定のご案内

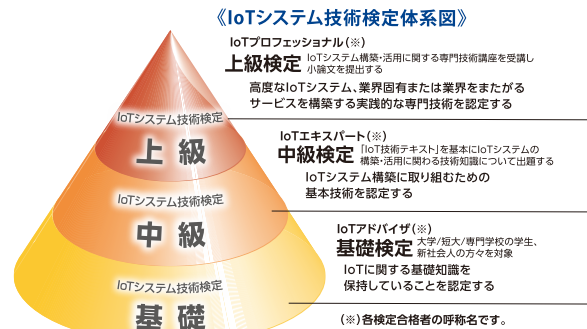
モバイルシステム技術検定

モバイルシステムを構成するワイヤレス通信、モバイル端末、モバイルコンテンツとアプリケーション、セキュリティ等の基本技術からモバイルシステム分析、構築などの応用技術までを体系化した4レベル資格の検定制度です。既に7万6千人以上が受検されモバイルシステム分野の「業界標準資格」です。



IoTシステム技術検定

IoTシステム構成と構築技術、センサ・アクチュエータと通信方式、データのAI分析と活用技術、IoTセキュリティ、プロトタイピングなどIoTシステムの概要と実務の基礎を体系化した3レベル資格の検定制度です。新ビジネスイノベーションの推進やIoT・AIで活躍される技術者の必須資格です。



New!! ワイヤレスIoTプランナー検定 認定研修/検定試験(CBT)

業界をリードするトップが推薦!



株式会社NTTドコモ
代表取締役社長
井伊 基之 氏



KDDI株式会社
代表取締役社長
高橋 誠氏



ソフトバンクグループ株式会社
代表取締役会長 兼 社長
孫 正義 氏



東京大学大学院工学系研究科教授
スマートIoT推進フォーラム
技術戦略検討部会長
森川 博之 氏



東京工業大学
副学長 (国際連携担当)
高田 潤一 氏

2021年度検定予定日

〈最新情報はWebよりご確認ください〉

■スマートフォン・モバイル実務検定 (CBT方式)

2021年 6月 1日(火)~ 6月18日(金)
2022年 2月14日(月)~ 3月 2日(水)

■モバイル技術基礎検定 (CBT方式)

2021年 6月 7日(月)~ 6月25日(金)
2022年 2月21日(月)~ 3月10日(木)

■モバイルシステム技術検定 [1級]

2021年 6月12日(土)
2021年 11月13日(土)

■モバイルシステム技術検定 [2級]

2021年 6月12日(土)
2021年 下期(別途) (CBT方式)

■SMC(シニアモバイルシステムコンサルタント)認定・更新研修

認定研修 2021年 9月17日(金)~18日(土)
更新研修 2021年 9月17日(金)、2022年3月11日(金)

■IoTシステム技術検定 [基礎・中級]

2021年 7月10日(土)
2021年 12月11日(土)

■IoTシステム技術検定 [上級] (2日間)

2021年 8月 6日(金)~ 8月 7日(土)
2022年 2月25日(金)~ 2月26日(土)

■ワイヤレスIoTプランナー検定 [基礎] 認定研修

2021年 6月26日(土)
2021年10月 2日(土)
2022年 2月 5日(土)

■ワイヤレスIoTプランナー検定 [基礎] (CBT方式)

2021年 7月1日(木)~ 7月16日(金)
2021年11月1日(月)~11月16日(火)
2022年 3月1日(金)~ 3月16日(火)

お申込み・詳細スケジュール等の検定についてはこちらへ

<https://www.mcpc-jp.org/license/index.htm>



KIOXIA

アトムよりも、お茶の水博士に憧れた そんな人間たちの集まりだから、 今日も夢中で未来を作りつづける

10万馬力のロボットより、それを作り出す技術者は逆境に強い
壁にぶつかることなど、日常茶飯事だからだ

100年に1度と言われる変化の時代でも、キオクシアは立ち止まらない
フラッシュメモリのインベンターのDNAを継ぎ、いまメモリをさらに進化させる

かつて子どもの頃に夢見た、ワクワクする技術を実現するために

今日も、私たちはよりよい未来を作りつづける

「記憶」で世界をおもしろくする



©TEZUKA PRODUCTIONS

2021年度

キオクシア奨励研究募集

理学・工学の更なる学術的発展に寄与することを目的としたプログラム

対象者	国内の学術研究機関に所属する研究者
研究対象	次世代メモリ・半導体技術・情報処理・AI関連技術(画像認識, テキストマイニング, 最適化などを含む)・DX関連技術(ビッグデータ, デジタルツイン)・アプリケーション・セキュリティ・圧縮・半導体回路設計・デバイス・プロセス・シミュレーション技術等の独創的なテーマ (Feasibility Study 含む)
研究費	100万円まで(間接経費、消費税等別)
採択数	20件予定 *2020年度採択実績: 23件
研究期間	契約締結より2022年3月31日まで
応募締切	2021年4月15日(木) 15時必着 応募書類による書類審査により2021年5月末までに決定予定

優れた成果を挙げた研究テーマを表彰いたします。

採択テーマは、当社との共同研究として翌年度以降の継続を検討する場合があります。

詳細はこちら ▶ <https://about.kioxia.com/ja-jp/news/2021/20210301-1.html>

キオクシア株式会社

技術改革推進部 産学連携事務局
kioxiahq-sangakuOffice@kioxia.com



〒101-0062 東京都千代田区神田駿河台一丁目五番

東京千代田区神田駿河台一丁目五番
発行所 一般社団法人 情報処理学会
発行人 木下泰三

電話 東京(03)35118183
振替口座 00015014183484

東京都荒川区西日暮里五丁目一丁目
印刷所 三美印刷株式会社

会員外発売所 東京都千代田区神田錦町三丁目一丁目

定価 1,760円 (本体 1,600円 + 税 10%)

本誌広告一手取扱い アドコム・メディア株式会社

〒169-0073 東京都新宿区百人町 2-21-27 TEL.03-3367-0571 FAX.03-3368-1519

雑誌 05269-04



4910052690417
01600